US009629060B2

(12) **United States Patent**
Arora et al.

(10) **Patent No.: US 9,629,060 B2**
(45) **Date of Patent: Apr. 18, 2017**

(54) **FLEXIBLE ROUTING POLICY FOR WI-FI OFFLOADED CELLULAR DATA**

(71) Applicant: **ORACLE INTERNATIONAL CORPORATION**, Redwood Shores, CA (US)

(72) Inventors: **Jitender Arora**, Nashua, NH (US); **Cheng Liu**, Acton, MA (US); **Nan Luo**, Shrewsbury, MA (US)

(73) Assignee: **Oracle International Corporation**, Redwood Shores, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 183 days.

(21) Appl. No.: **14/298,405**

(22) Filed: **Jun. 6, 2014**

(65) **Prior Publication Data**

US 2015/0358889 A1 Dec. 10, 2015

(51) **Int. Cl.**

H04W 40/18	(2009.01)
H04W 40/04	(2009.01)
H04W 4/18	(2009.01)
H04W 76/02	(2009.01)
H04W 88/08	(2009.01)
H04W 88/16	(2009.01)
H04W 88/12	(2009.01)
H04W 84/12	(2009.01)

(52) **U.S. Cl.**

CPC ***H04W 40/04*** (2013.01); ***H04W 4/18*** (2013.01); ***H04W 76/022*** (2013.01); *H04W 84/12* (2013.01); *H04W 88/08* (2013.01); *H04W 88/12* (2013.01); *H04W 88/16* (2013.01)

(58) **Field of Classification Search**

None

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

8,204,064	B2	6/2012	MeLampy et al.	
8,457,130	B2	6/2013	Kumar et al.	
8,554,142	B2	10/2013	Hoover et al.	
8,934,453	B1 *	1/2015	Sarnaik	H04W 76/022 370/331
9,277,592	B2 *	3/2016	Zhou	H04M 15/66
2011/0019644	A1 *	1/2011	Cheon	H04W 36/0033 370/331
2012/0246325	A1 *	9/2012	Pancorbo Marcos	H04L 12/2602 709/227

(Continued)

OTHER PUBLICATIONS

Kyunghan Lee et al.; "Mobile Data Offloading: How Much Can WiFi Deliver?"; ACM CoNEXT 2010, Nov. 30-Dec. 3 2010, Philadelphia, USA.

(Continued)

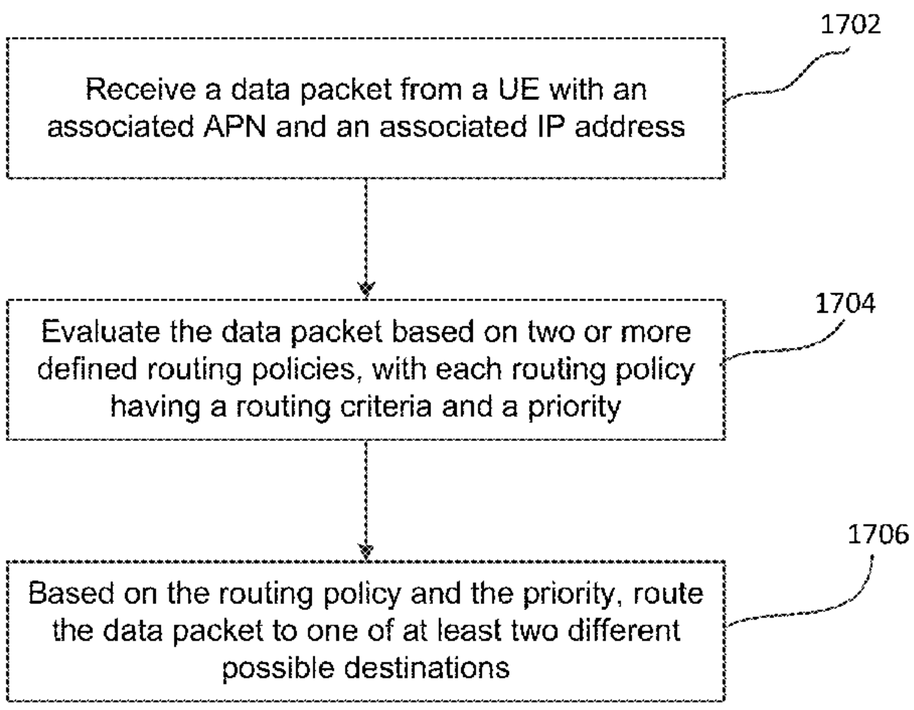
Primary Examiner — Bunjob Jaroenchonwanit

(74) *Attorney, Agent, or Firm* — Miles & Stockbridge P.C.

(57) **ABSTRACT**

A system/router that flexibly routes Wi-Fi offloaded data receives a data packet from a user equipment via an access point of a Wi-Fi network. The data packet includes an access point name ("APN") and an Internet Protocol ("IP") address. The system defines two or more routing policies, each routing policy including a routing criteria and a priority. The system evaluates the data packet based on the routing policies, and routes the data packet to one of at least two possible destinations based at least on the routing policies, including the priorities.

20 Claims, 17 Drawing Sheets



(56) **References Cited**

U.S. PATENT DOCUMENTS

2013/0077482	A1	3/2013	Krishna et al.	
2013/0100955	A1*	4/2013	Dunlap	H04L 47/20 370/392
2013/0138823	A1	5/2013	Centemeri et al.	
2013/0223421	A1*	8/2013	Gundavelli	H04W 76/022 370/338
2014/0086177	A1*	3/2014	Adjakple	H04W 12/08 370/329
2014/0092899	A1*	4/2014	Krishna	H04L 61/2517 370/389
2014/0119340	A1*	5/2014	Stojanovski	H04W 8/082 370/331
2014/0161026	A1*	6/2014	Stojanovski	H04L 45/22 370/328
2014/0192651	A1*	7/2014	Sun	H04L 45/38 370/235
2014/0380434	A1*	12/2014	Li	H04W 4/24 726/4
2016/0087932	A1*	3/2016	Hergenhan	H04L 12/6418 709/218
2017/0026824	A1*	1/2017	Kim	H04W 8/08

OTHER PUBLICATIONS

Oracle Data Sheet; "Oracle Communications Security Gateway"; copyright 2013, last downloaded Jun. 6, 2014.

* cited by examiner

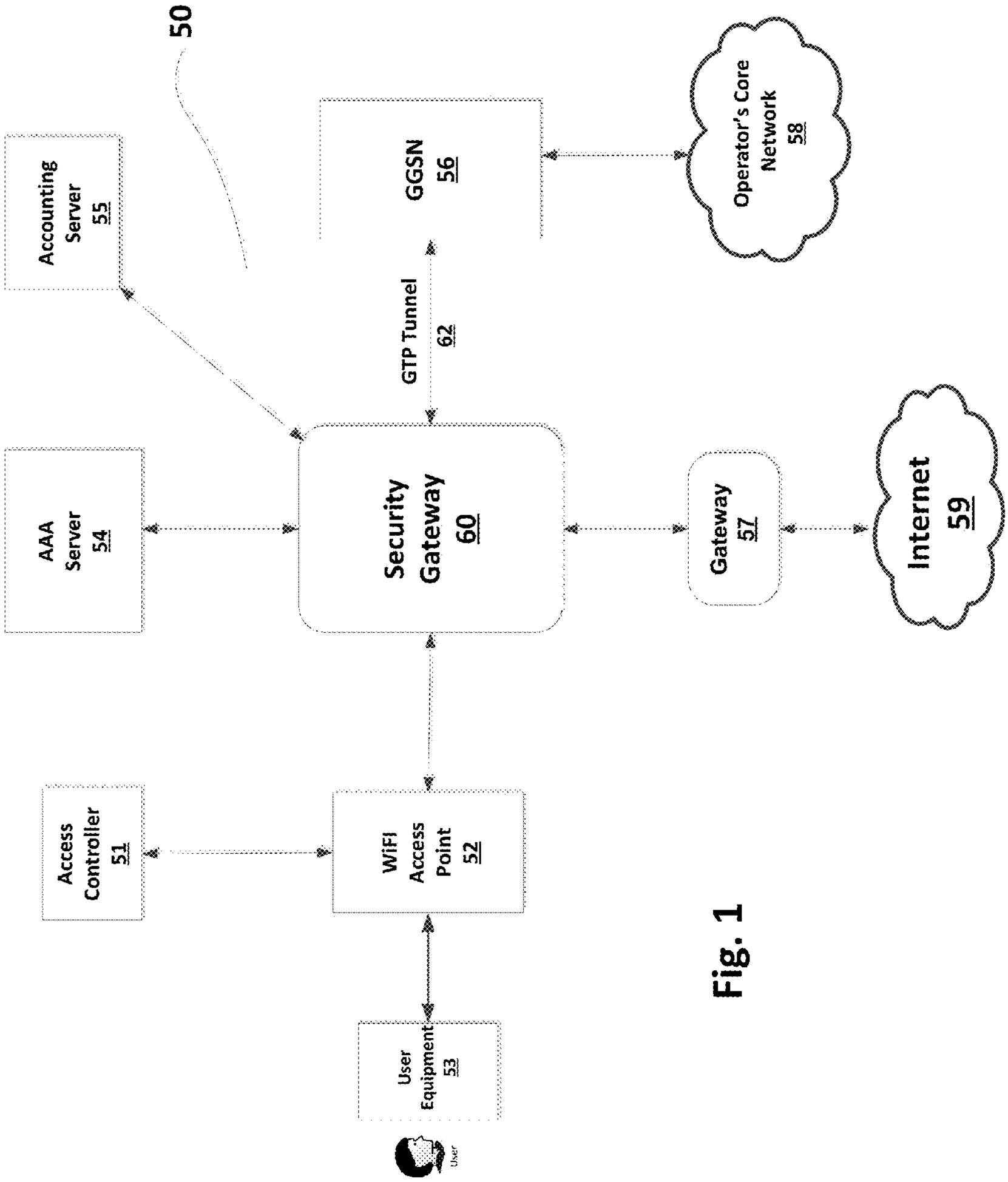

50
Accounting Server 55
GGSN 56
Operator's Core Network 58
GTP Tunnel 62
AAA Server 54
Security Gateway 60
Gateway 57
Internet 59
Access Controller 51
WiFi Access Point 52
User Equipment 53
User

Fig. 1

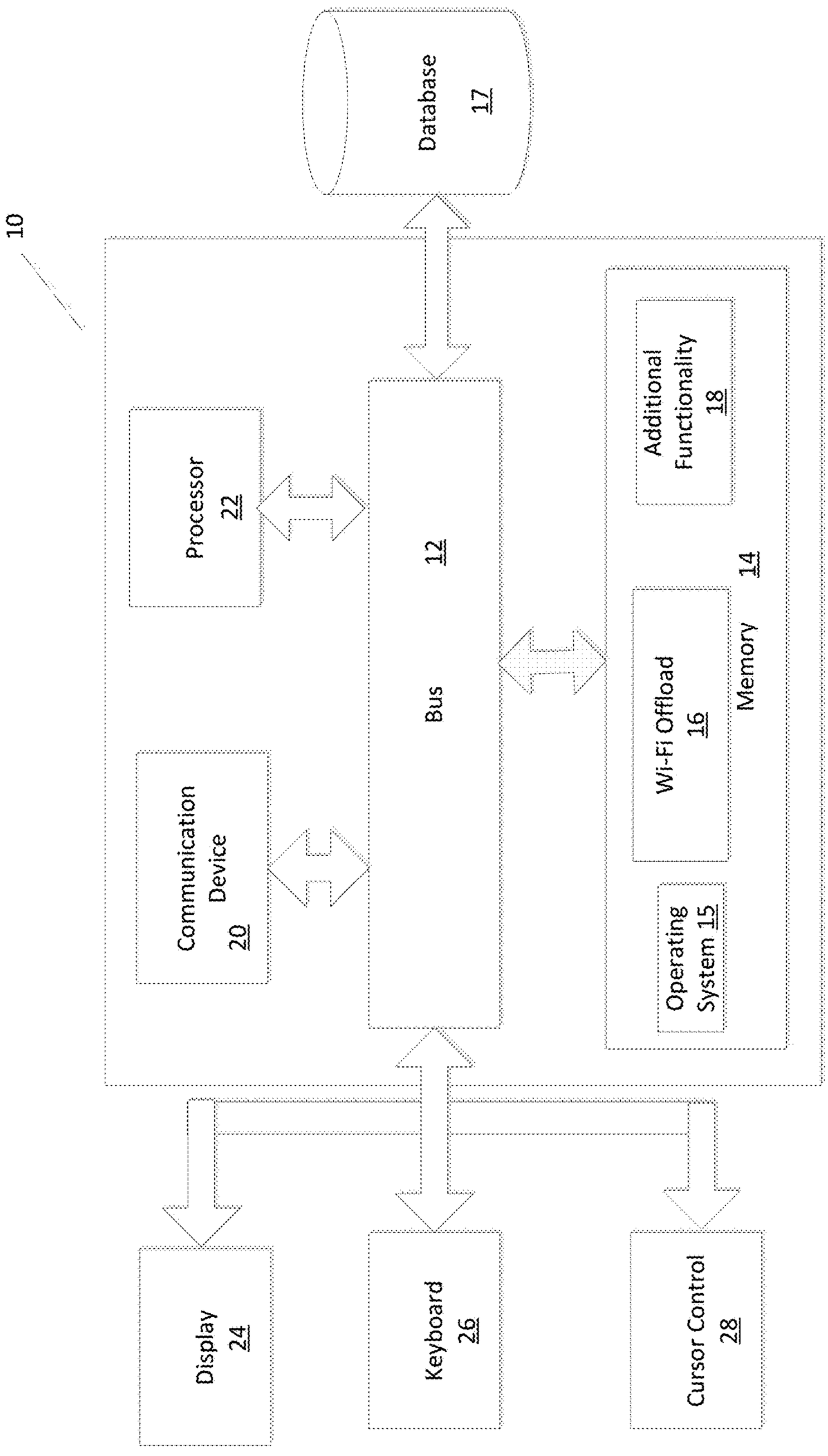

Database 17
10
Processor 22
Bus 12
Communication Device 20
Additional Functionality 18
Wi-Fi Offload 16
Memory 14
Operating System 15
Display 24
Keyboard 26
Cursor Control 28

Fig. 2

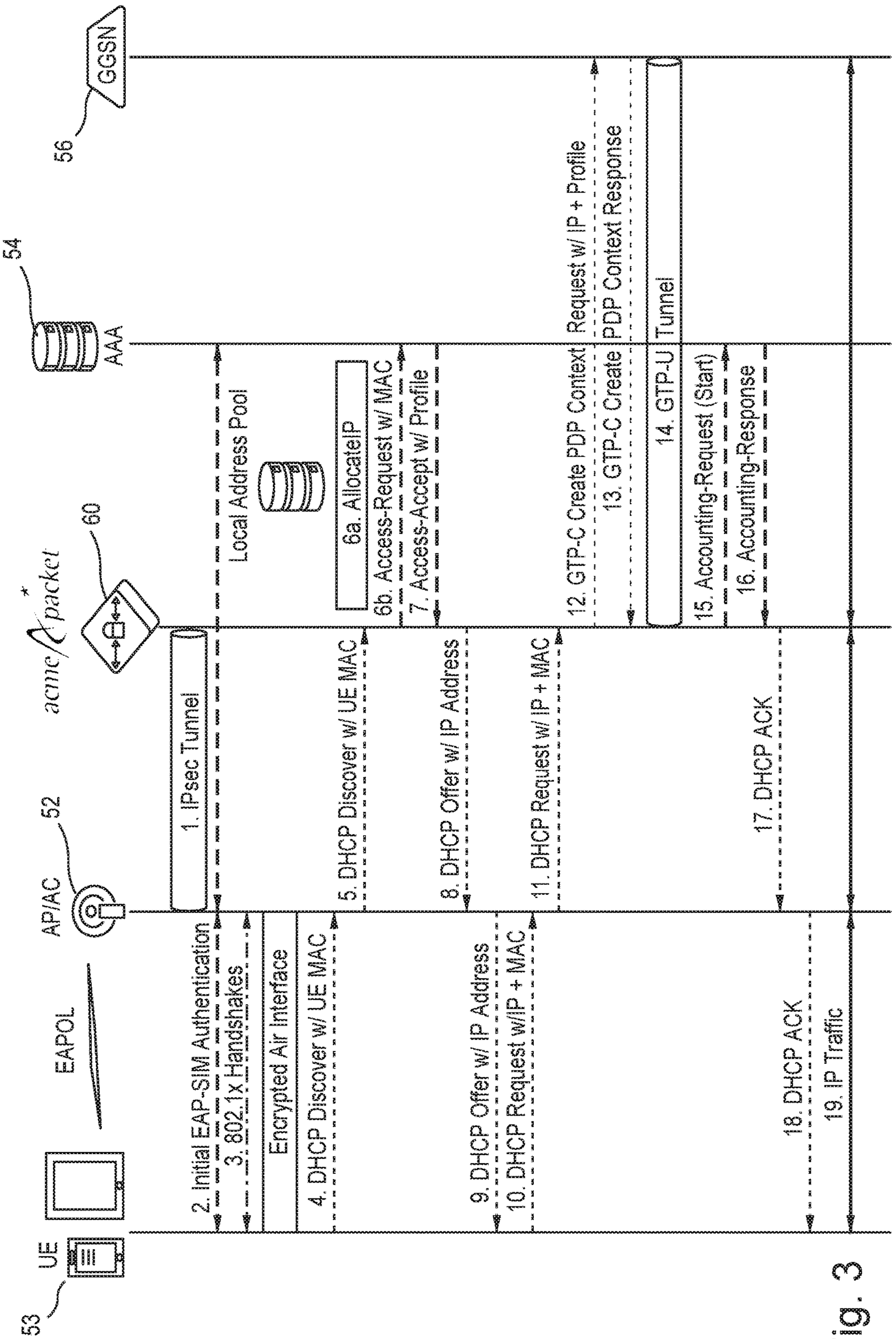

GGSN
56
AAA
60
acme packet
Local Address Pool
AP/AC
52
EAPOL
UE
53
54
1. IPsec Tunnel
2. Initial EAP-SIM Authentication
3. 802.1x Handshakes
Encrypted Air Interface
4. DHCP Discover w/ UE MAC
5. DHCP Discover w/ UE MAC
6a. AllocateIP
6b. Access-Request w/ MAC
7. Access-Accept w/ Profile
8. DHCP Offer w/ IP Address
9. DHCP Offer w/ IP Address
10. DHCP Request w/IP + MAC
11. DHCP Request w/ IP + MAC
12. GTP-C Create PDP Context Request w/ IP + Profile
13. GTP-C Create PDP Context Response
14. GTP-U Tunnel
15. Accounting-Request (Start)
16. Accounting-Response
17. DHCP ACK
18. DHCP ACK
19. IP Traffic

Fig. 3

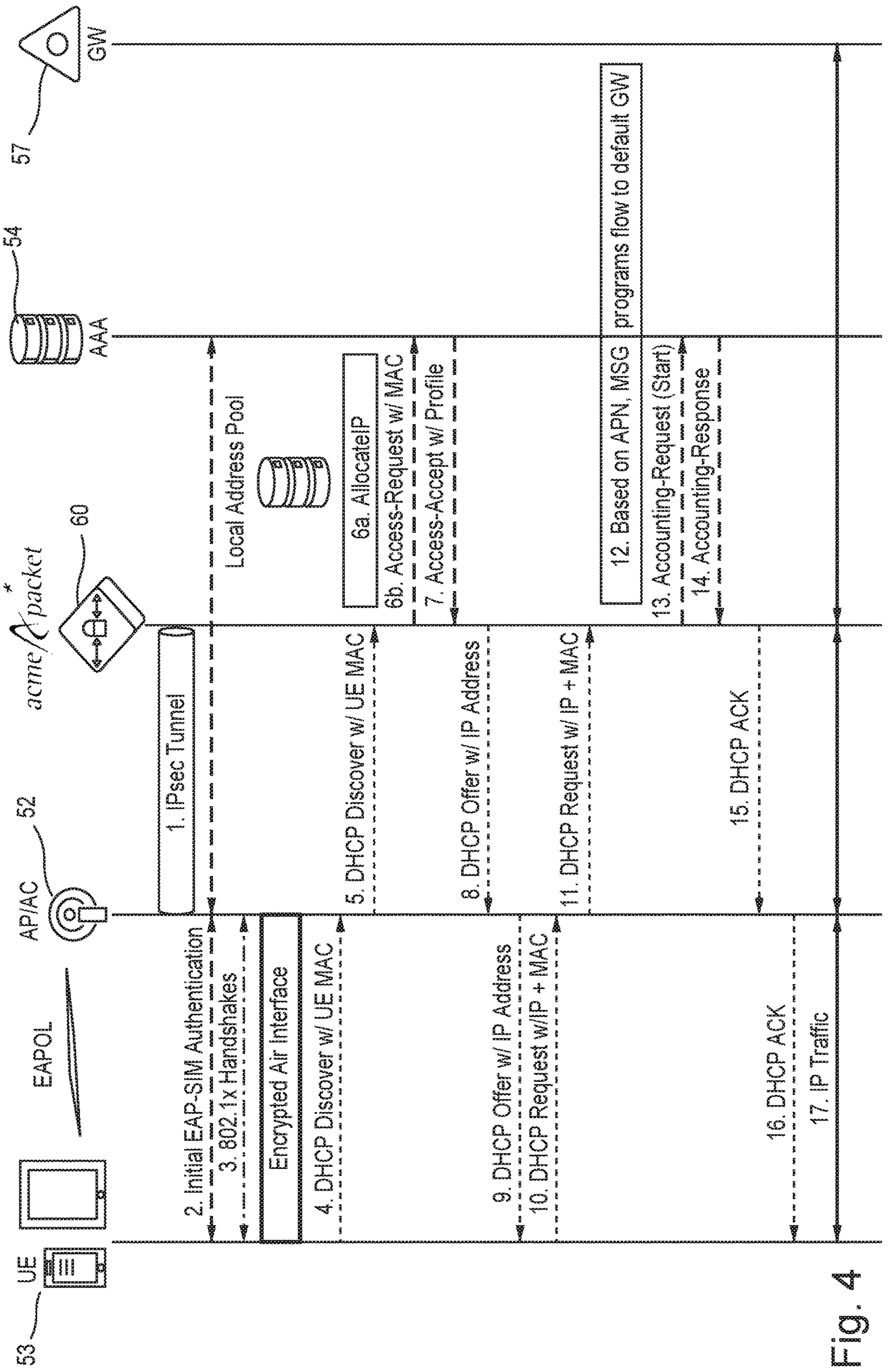

GW
57
54
AAA
acme packet
60
AP/AC
52
EAPOL
UE
53
1. IPsec Tunnel
Local Address Pool
2. Initial EAP-SIM Authentication
3. 802.1x Handshakes
Encrypted Air Interface
4. DHCP Discover w/ UE MAC
5. DHCP Discover w/ UE MAC
6a. AllocateIP
6b. Access-Request w/ MAC
7. Access-Accept w/ Profile
8. DHCP Offer w/ IP Address
9. DHCP Offer w/ IP Address
10. DHCP Request w/IP + MAC
11. DHCP Request w/ IP + MAC
12. Based on APN, MSG programs flow to default GW
13. Accounting-Request (Start)
14. Accounting-Response
15. DHCP ACK
16. DHCP ACK
17. IP Traffic

Fig. 4

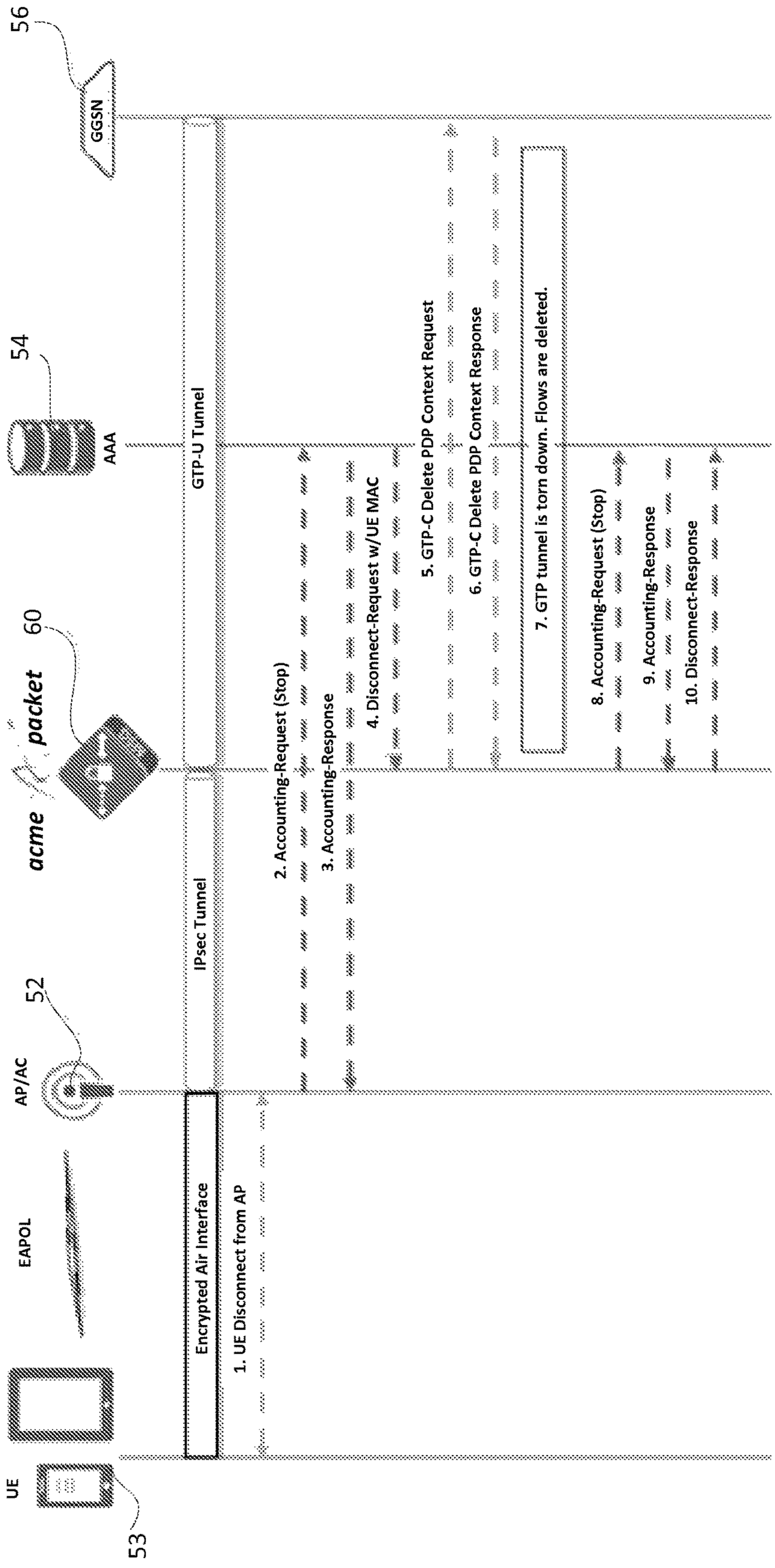

56
GGSN
54
AAA
acme packet
60
52
AP/AC
EAPOL
UE
53
IPsec Tunnel
GTP-U Tunnel
Encrypted Air Interface
1. UE Disconnect from AP
2. Accounting-Request (Stop)
3. Accounting-Response
4. Disconnect-Request w/UE MAC
5. GTP-C Delete PDP Context Request
6. GTP-C Delete PDP Context Response
7. GTP tunnel is torn down. Flows are deleted.
8. Accounting-Request (Stop)
9. Accounting-Response
10. Disconnect-Response

Fig. 5

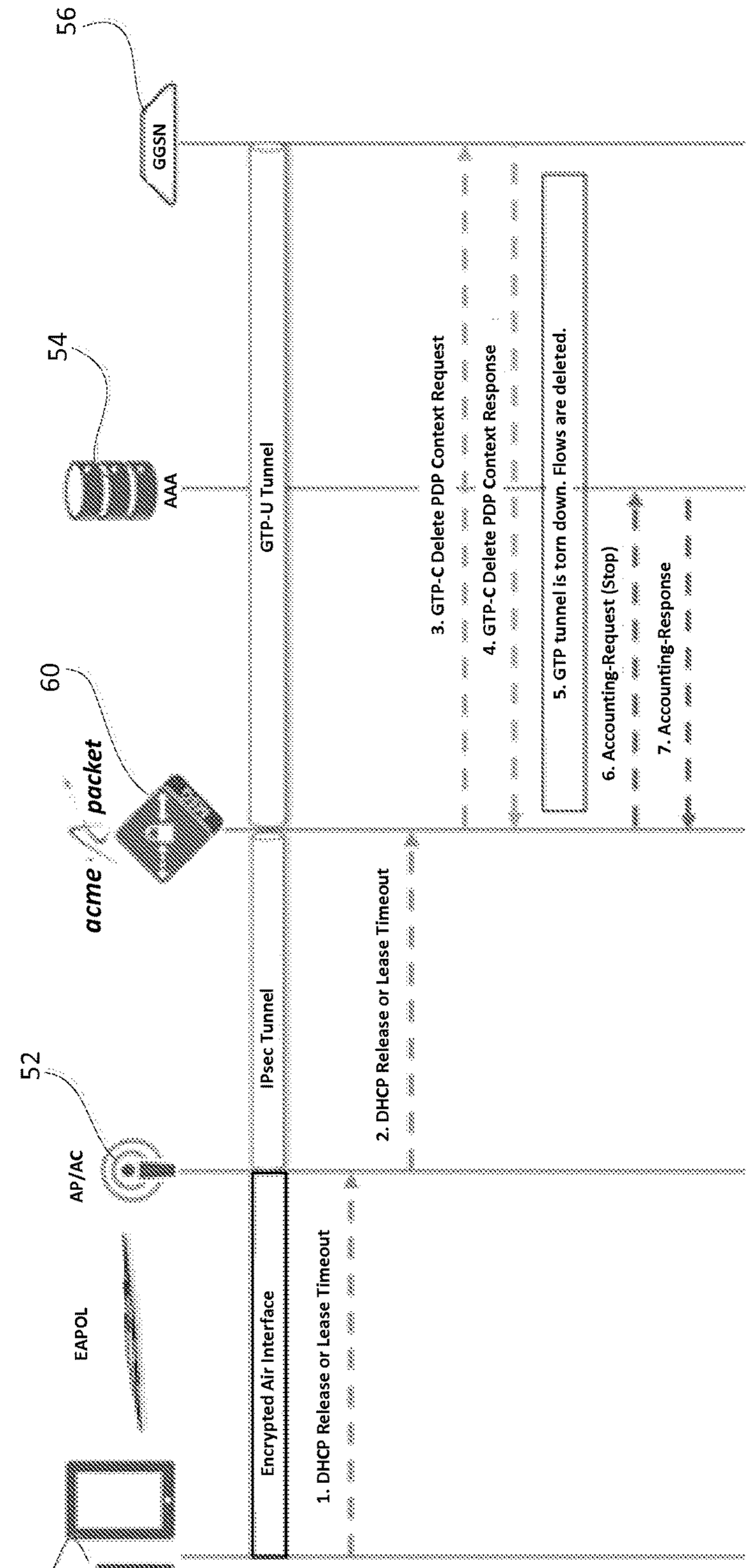

56
GGSN
54
AAA
60
acme packet
52
AP/AC
EAPOL
UE
53
IPsec Tunnel
GTP-U Tunnel
Encrypted Air Interface
1. DHCP Release or Lease Timeout
2. DHCP Release or Lease Timeout
3. GTP-C Delete PDP Context Request
4. GTP-C Delete PDP Context Response
5. GTP tunnel is torn down. Flows are deleted.
6. Accounting-Request (Stop)
7. Accounting-Response

Fig. 6

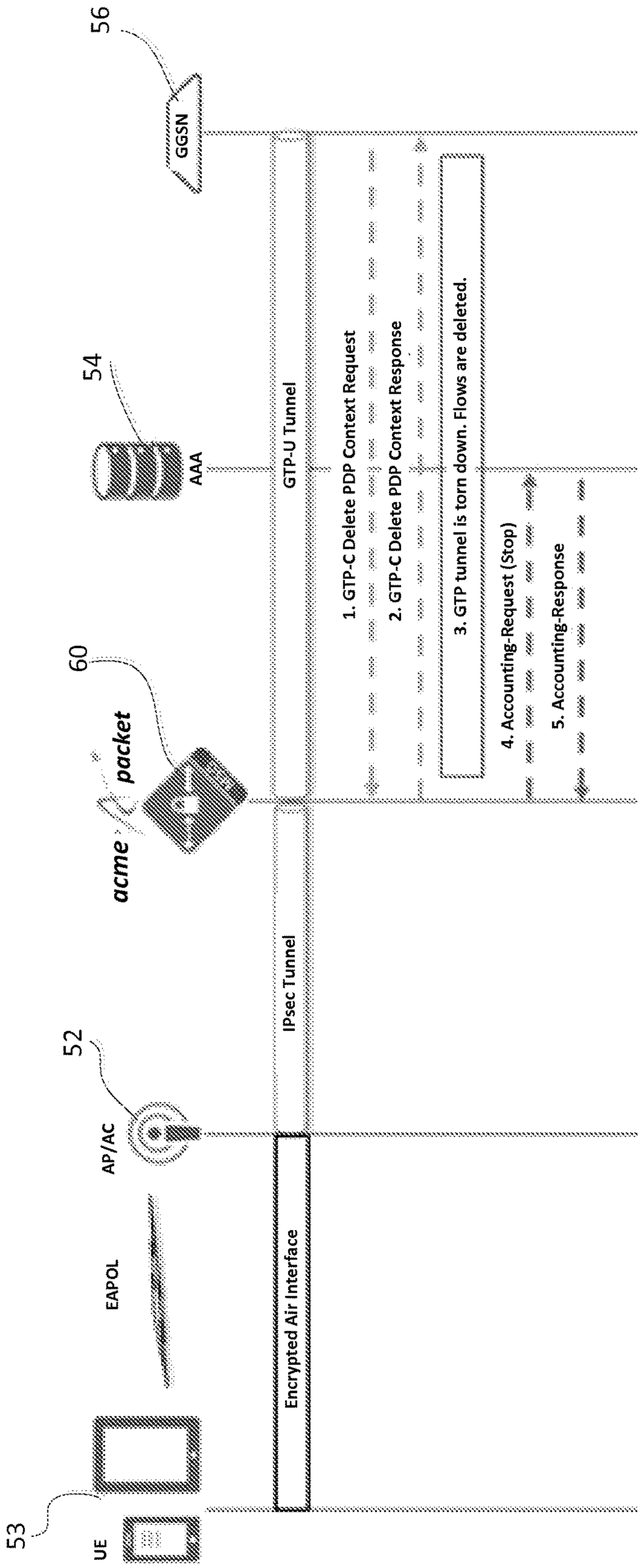

56
GGSN
54
AAA
60
acme packet
52
AP/AC
EAPOL
53
UE
IPsec Tunnel
Encrypted Air Interface
GTP-U Tunnel
1. GTP-C Delete PDP Context Request
2. GTP-C Delete PDP Context Response
3. GTP tunnel is torn down. Flows are deleted.
4. Accounting-Request (Stop)
5. Accounting-Response

Fig. 7

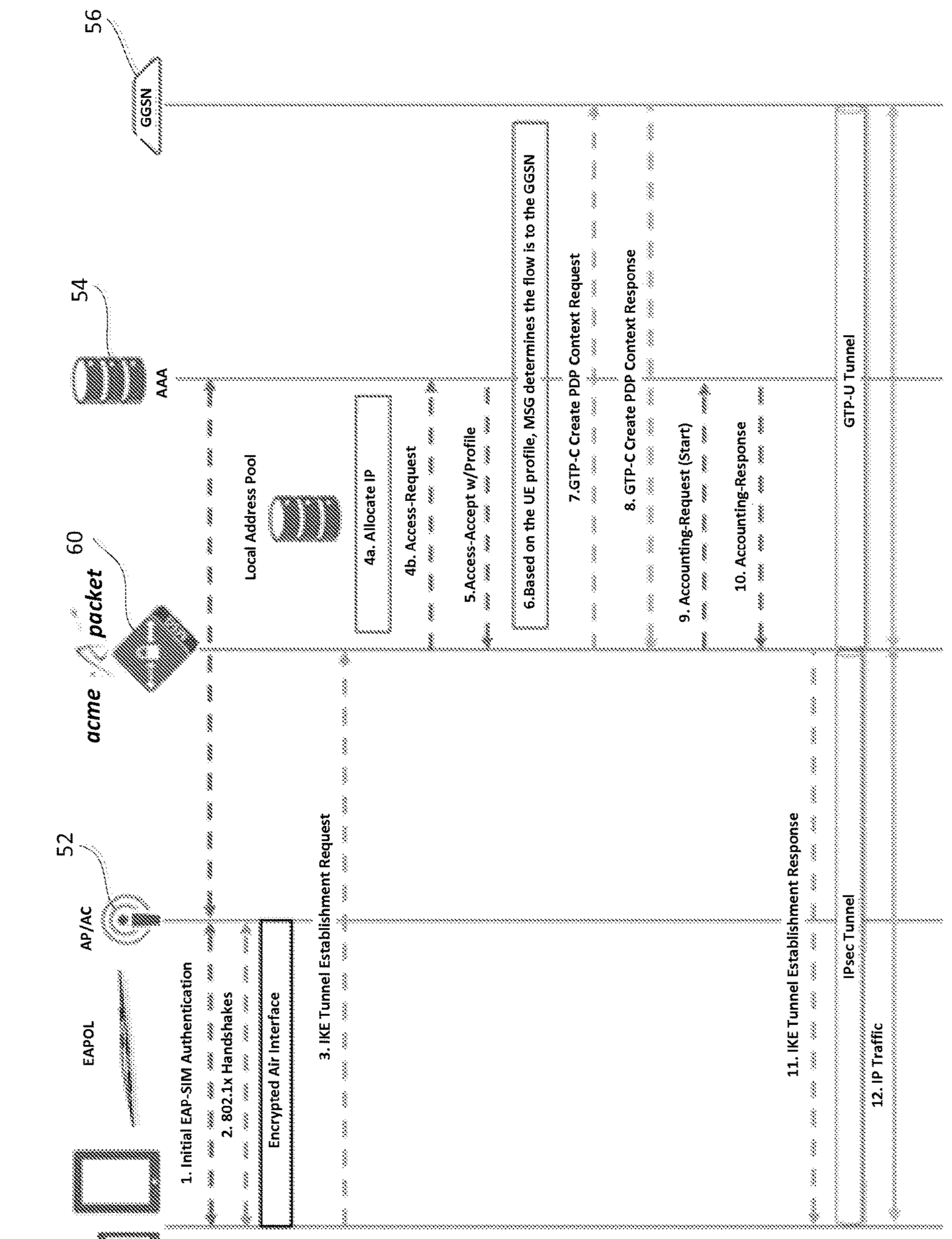

UE
53
AP/AC
52
acme packet
60
AAA
54
GGSN
56
EAPOL
1. Initial EAP-SIM Authentication
2. 802.1x Handshakes
Encrypted Air Interface
3. IKE Tunnel Establishment Request
Local Address Pool
4a. Allocate IP
4b. Access-Request
5.Access-Accept w/Profile
6.Based on the UE profile, MSG determines the flow is to the GGSN
7.GTP-C Create PDP Context Request
8. GTP-C Create PDP Context Response
9. Accounting-Request (Start)
10. Accounting-Response
11. IKE Tunnel Establishment Response
GTP-U Tunnel
IPsec Tunnel
12. IP Traffic

Fig. 8

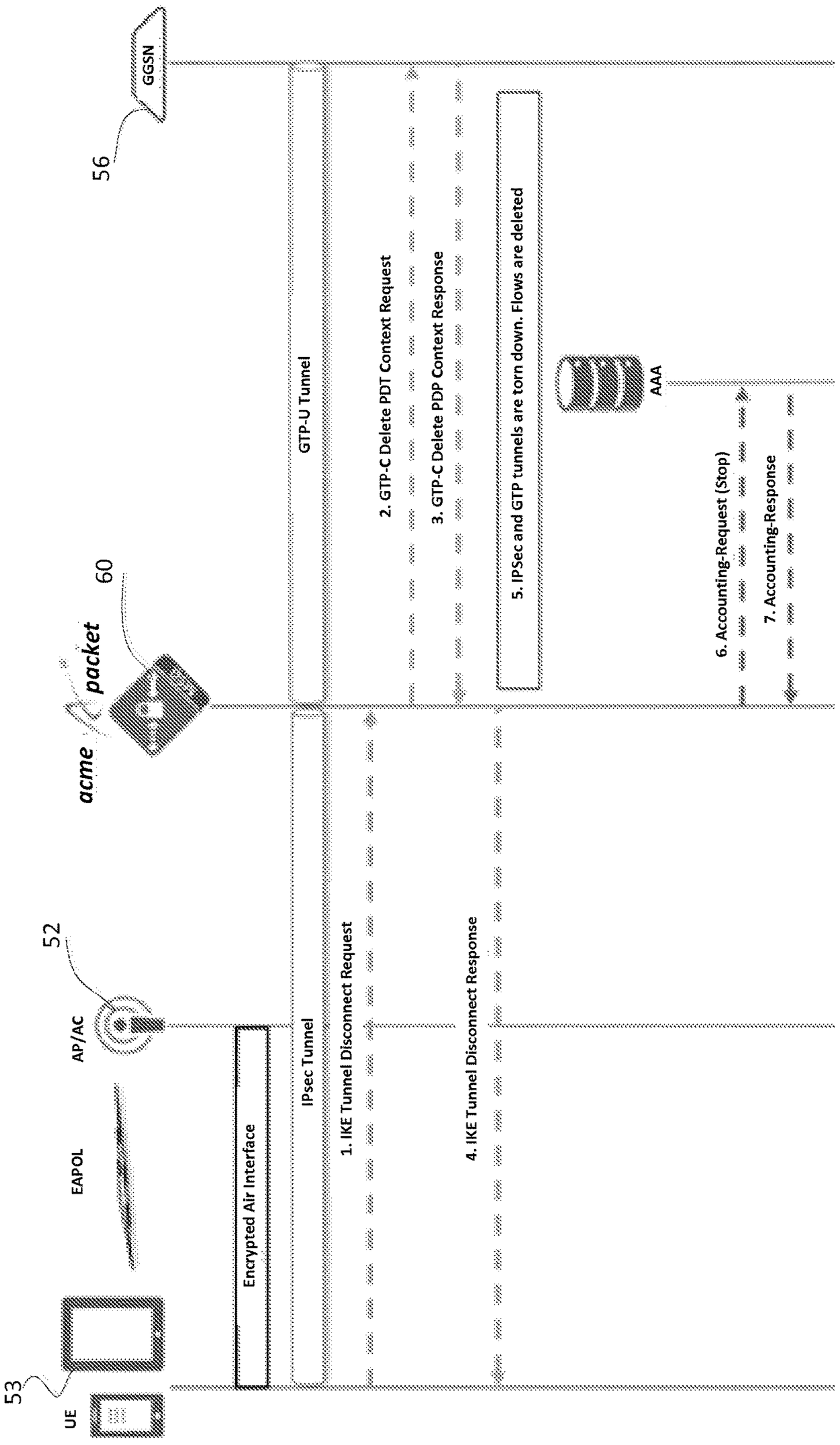

UE
53
EAPOL
AP/AC
52
acme packet
60
GGSN
56
AAA
Encrypted Air Interface
IPsec Tunnel
GTP-U Tunnel
1. IKE Tunnel Disconnect Request
4. IKE Tunnel Disconnect Response
2. GTP-C Delete PDT Context Request
3. GTP-C Delete PDP Context Response
5. IPSec and GTP tunnels are torn down. Flows are deleted
6. Accounting-Request (Stop)
7. Accounting-Response

Fig. 9

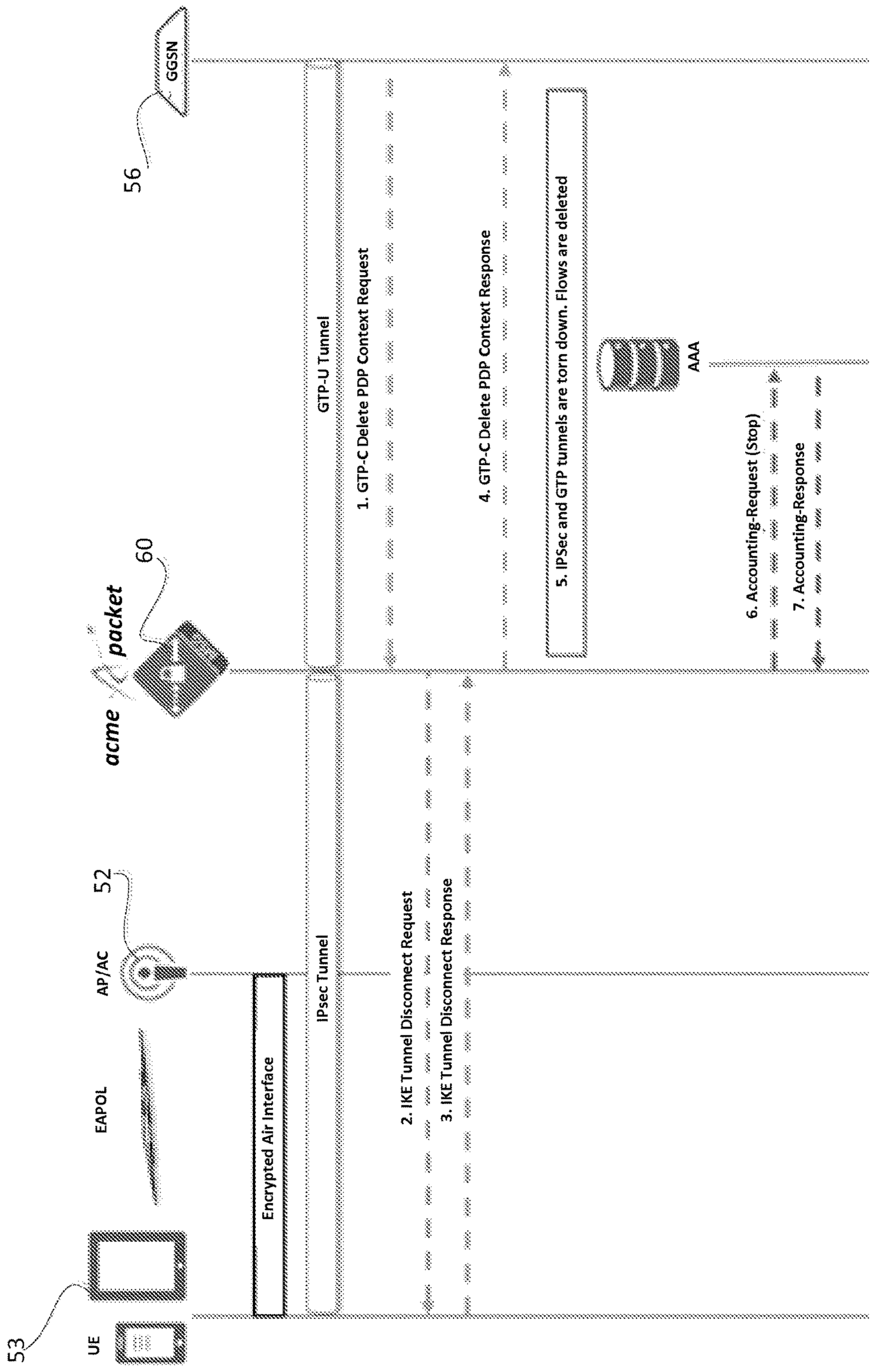

GGSN
56
acme packet
60
52
AP/AC
EAPOL
UE
53
Encrypted Air Interface
IPsec Tunnel
GTP-U Tunnel
1. GTP-C Delete PDP Context Request
2. IKE Tunnel Disconnect Request
3. IKE Tunnel Disconnect Response
4. GTP-C Delete PDP Context Response
5. IPSec and GTP tunnels are torn down. Flows are deleted
AAA
6. Accounting-Request (Stop)
7. Accounting-Response

Fig. 10

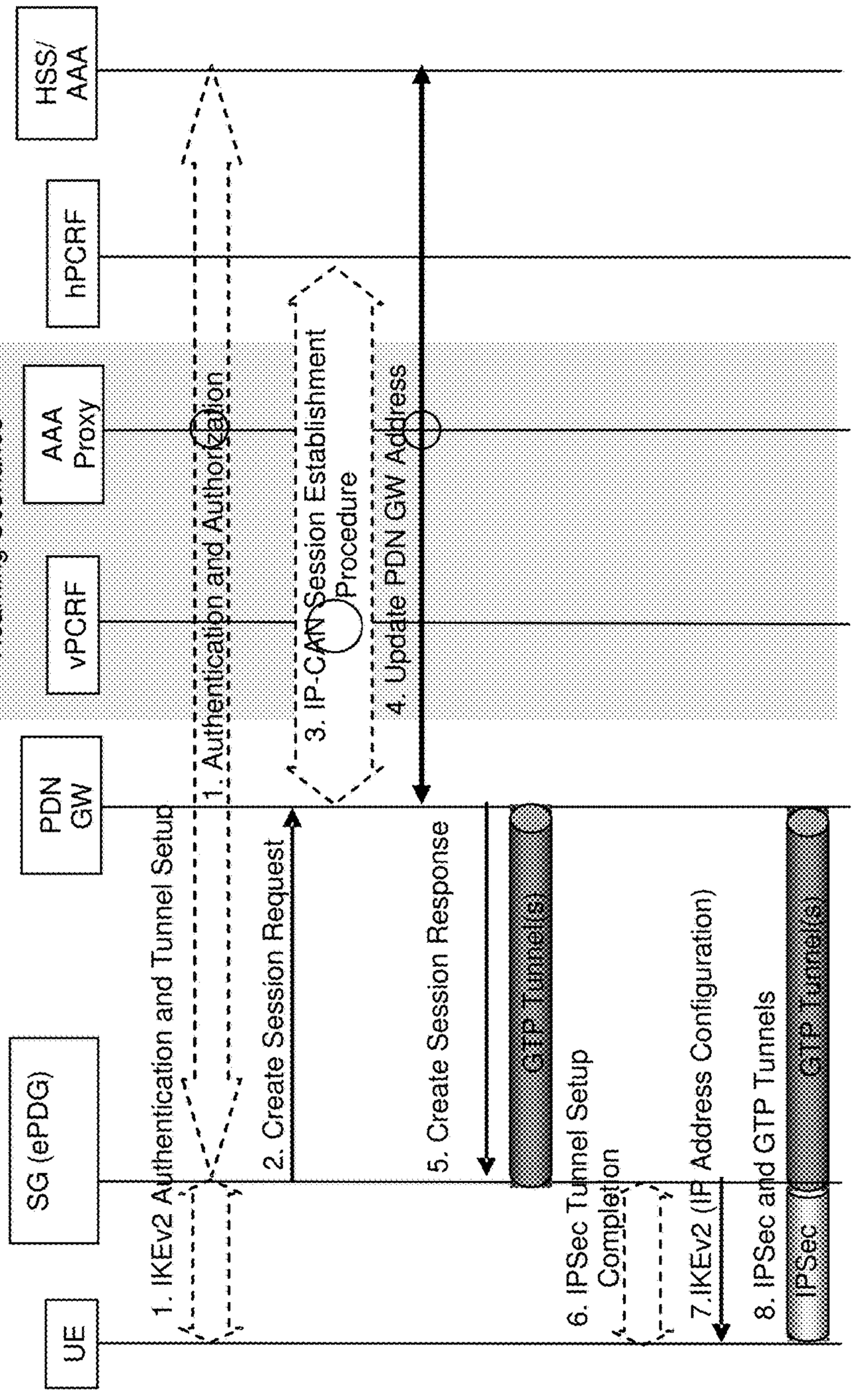

HSS/ AAA
hPCRF
Roaming Scenarios
AAA Proxy
vPCRF
PDN GW
1. Authentication and Authorization
3. IP-CAN Session Establishment Procedure
4. Update PDN GW Address
UE
SG (ePDG)
1. IKEv2 Authentication and Tu
2. Create Session
5. Create Session
6. IPSec Tunnel Setup Completion
7.IKEv2 (IP Address Configura
8. IPSec and GTP Tunnels
IPSec
GTP Tunn

Fig. 11

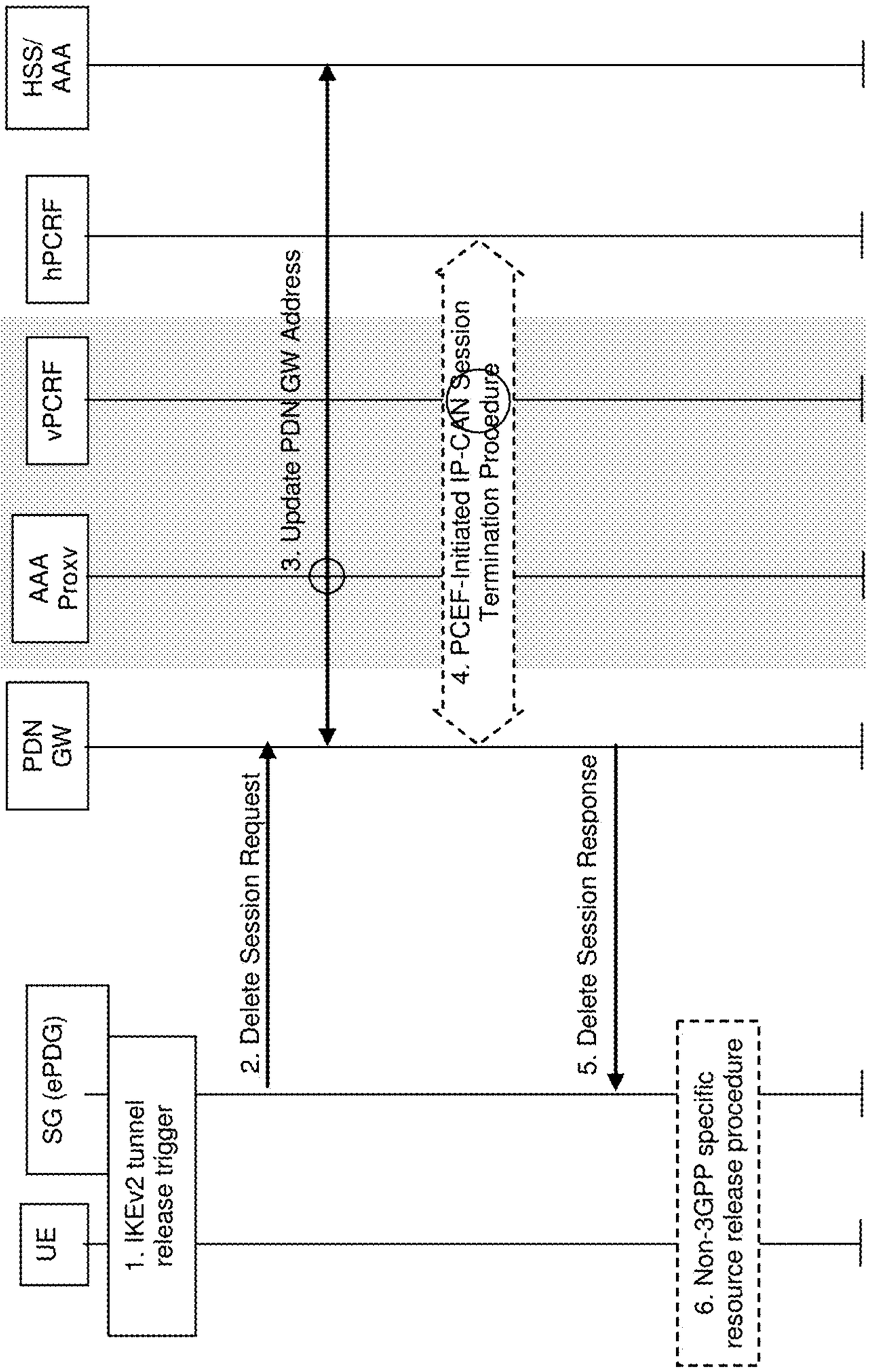

UE
SG (ePDG)
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
Roaming Scenarios
1. IKEv2 tunnel release trigger
2. Delete Session Request
3. Update PDN GW Address
4. PCEF-Initiated IP-CAN Session Termination Procedure
5. Delete Session Response
6. Non-3GPP specific resource release procedure

Fig. 12

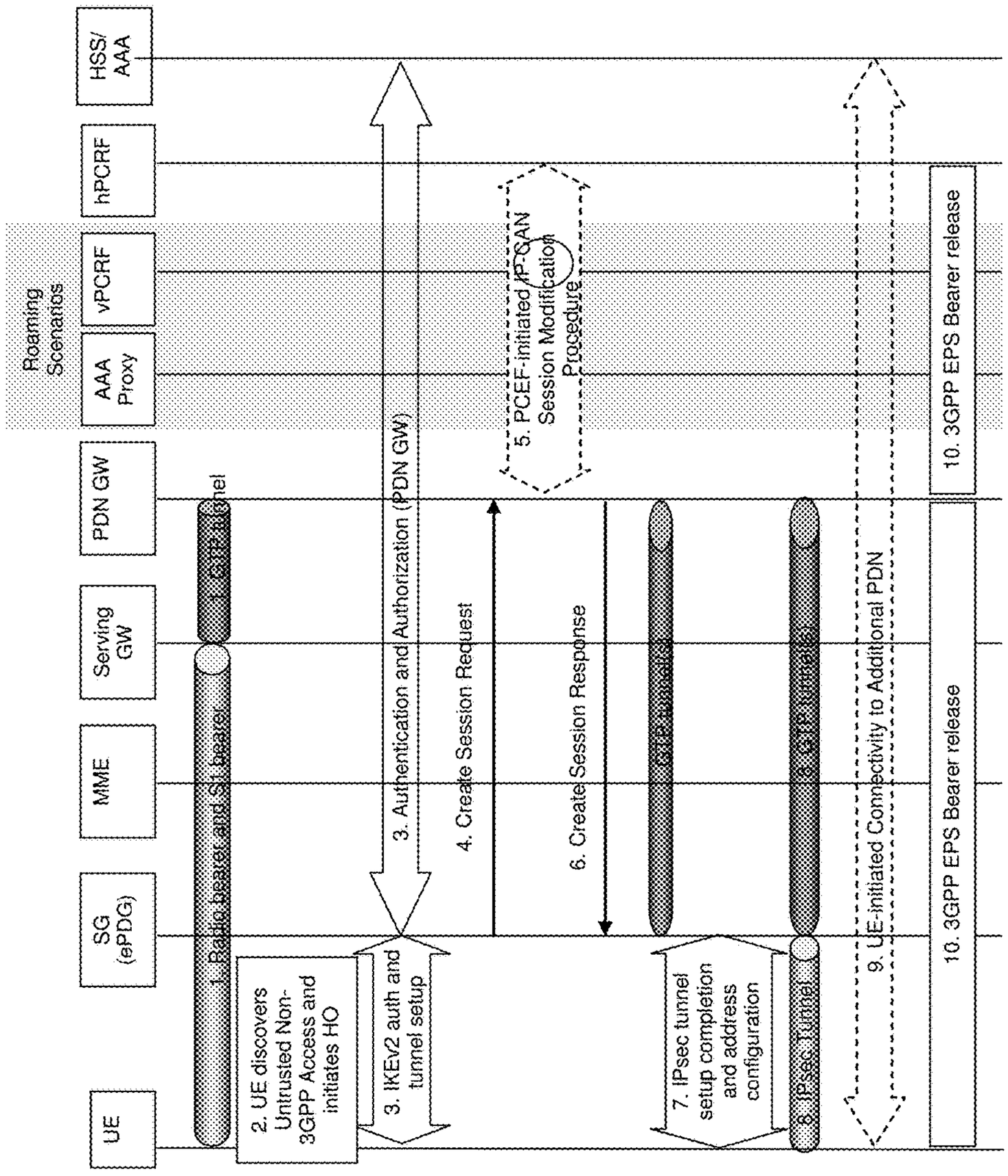

UE
SG (ePDG)
MME
Serving GW
PDN GW
Roaming Scenarios
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
1. Radio bearer and S1 bearer
1. GTP tunnel
2. UE discovers Untrusted Non-3GPP Access and initiates HO
3. IKEv2 auth and tunnel setup
3. Authentication and Authorization (PDN GW)
4. Create Session Request
5. PCEF-initiated IP-CAN Session Modification Procedure
6. Create Session Response
GTP tunnel
7. IPsec tunnel setup completion and address configuration
8. IPsec Tunnel
8. GTP tunnel
9. UE-initiated Connectivity to Additional PDN
10. 3GPP EPS Bearer release
10. 3GPP EPS Bearer release

Fig. 13

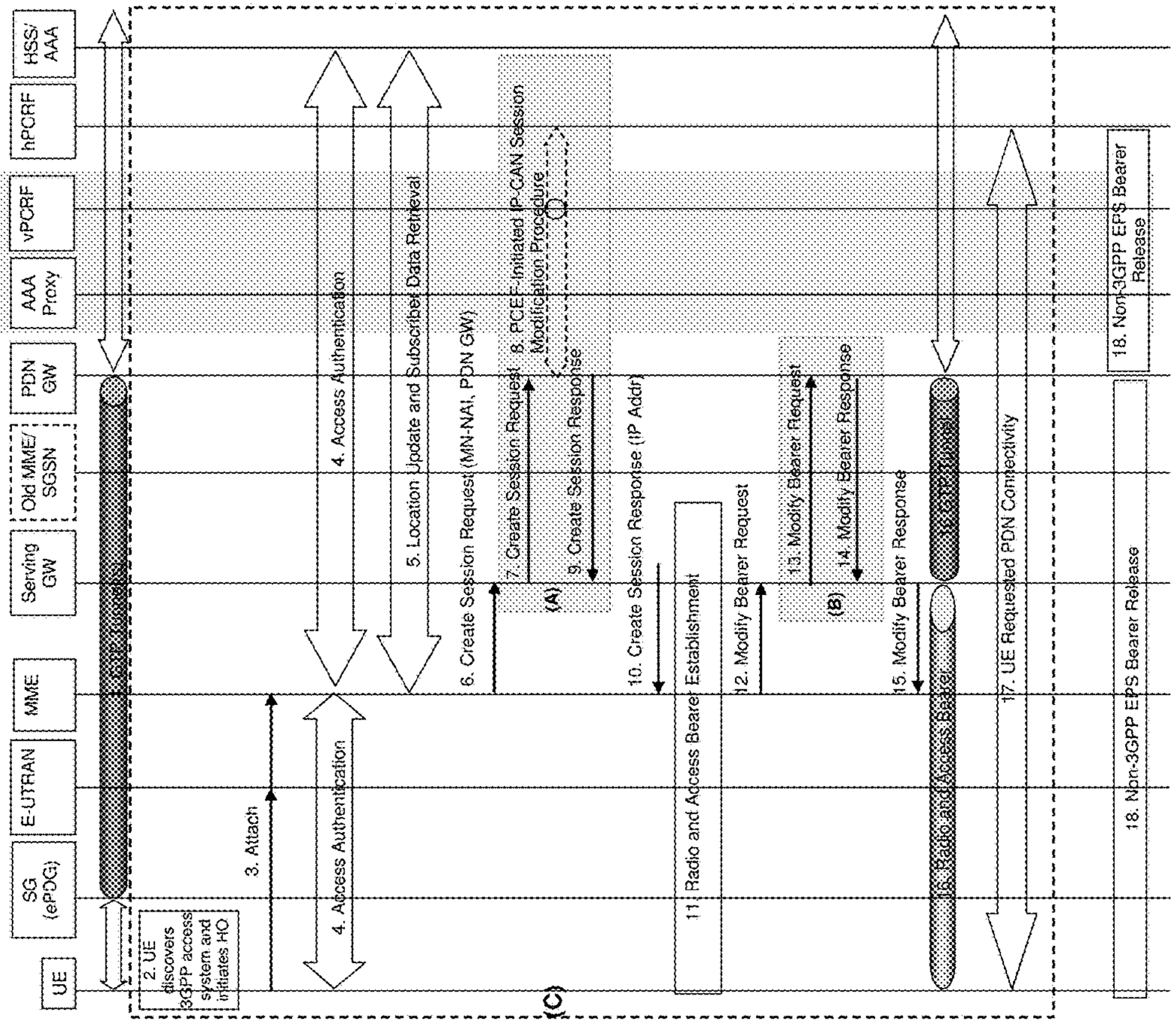

UE
SG (ePDG)
E-UTRAN
MME
Serving GW
Old MME/ SGSN
PDN GW
AAA Proxy
vPCRF
hPCRF
HSS/ AAA
Roaming Scenarios
1. PDN Connectivity
2. UE discovers 3GPP access system and initiates HO
3. Attach
4. Access Authentication
4. Access Authentication
5. Location Update and Subscriber Data Retrieval
6. Create Session Request (MN-NAI, PDN GW)
7. Create Session Request
8. PCEF-Initiated IP-CAN Session Modification Procedure
9. Create Session Response
(A)
10. Create Session Response (IP Addr)
11. Radio and Access Bearer Establishment
12. Modify Bearer Request
13. Modify Bearer Request
14. Modify Bearer Response
(B)
15. Modify Bearer Response
16. Radio and Access Bearer
17. UE Requested PDN Connectivity
18. Non-3GPP EPS Bearer Release
18. Non-3GPP EPS Bearer Release
(C)

Fig. 14

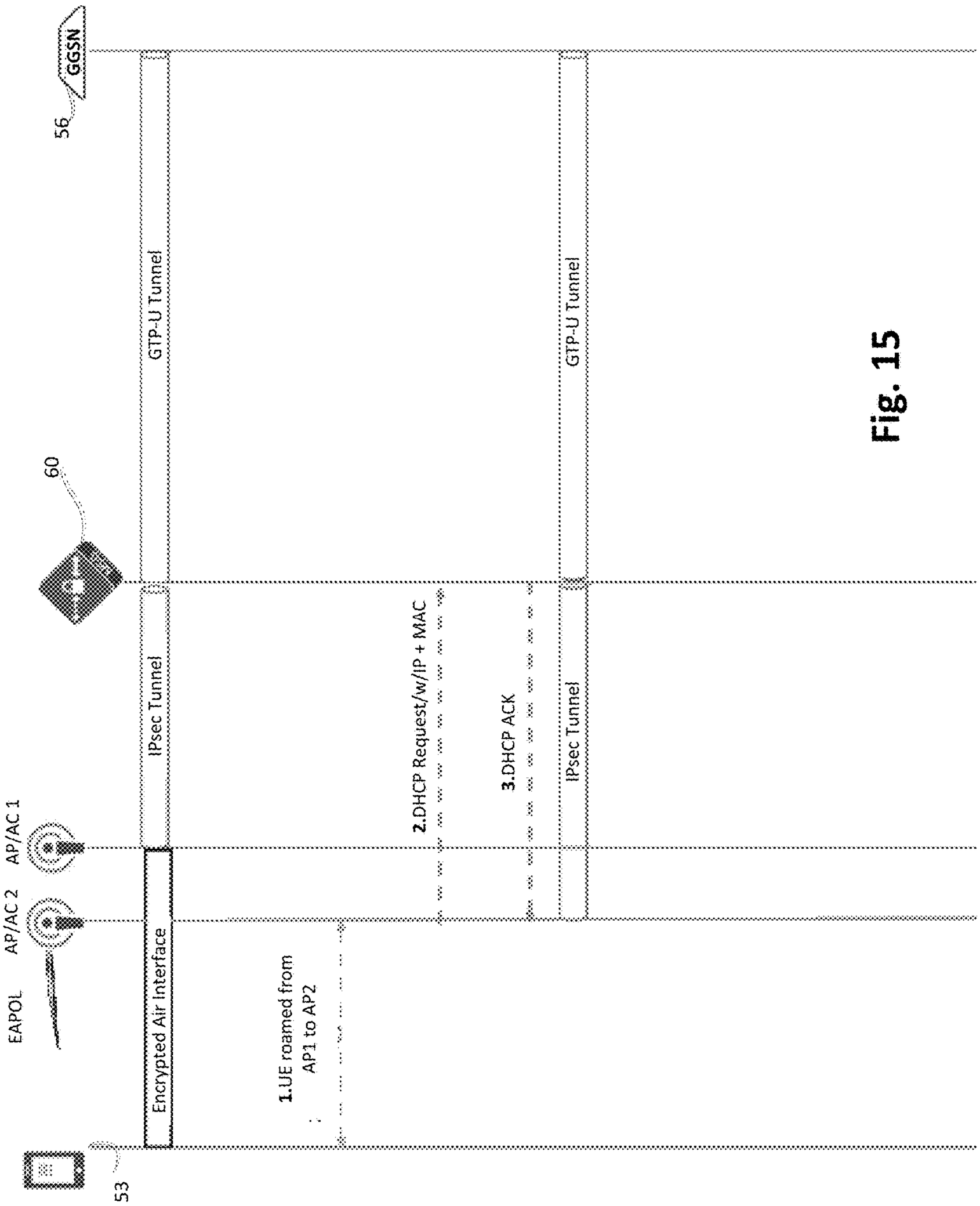

GGSN
56
IPsec Tunnel
GTP-U Tunnel
60
AP/AC 1
AP/AC 2
EAPOL
Encrypted Air Interface
1.UE roamed from AP1 to AP2
2.DHCP Request/w/IP + MAC
3.DHCP ACK
IPsec Tunnel
GTP-U Tunnel
53

Fig. 15

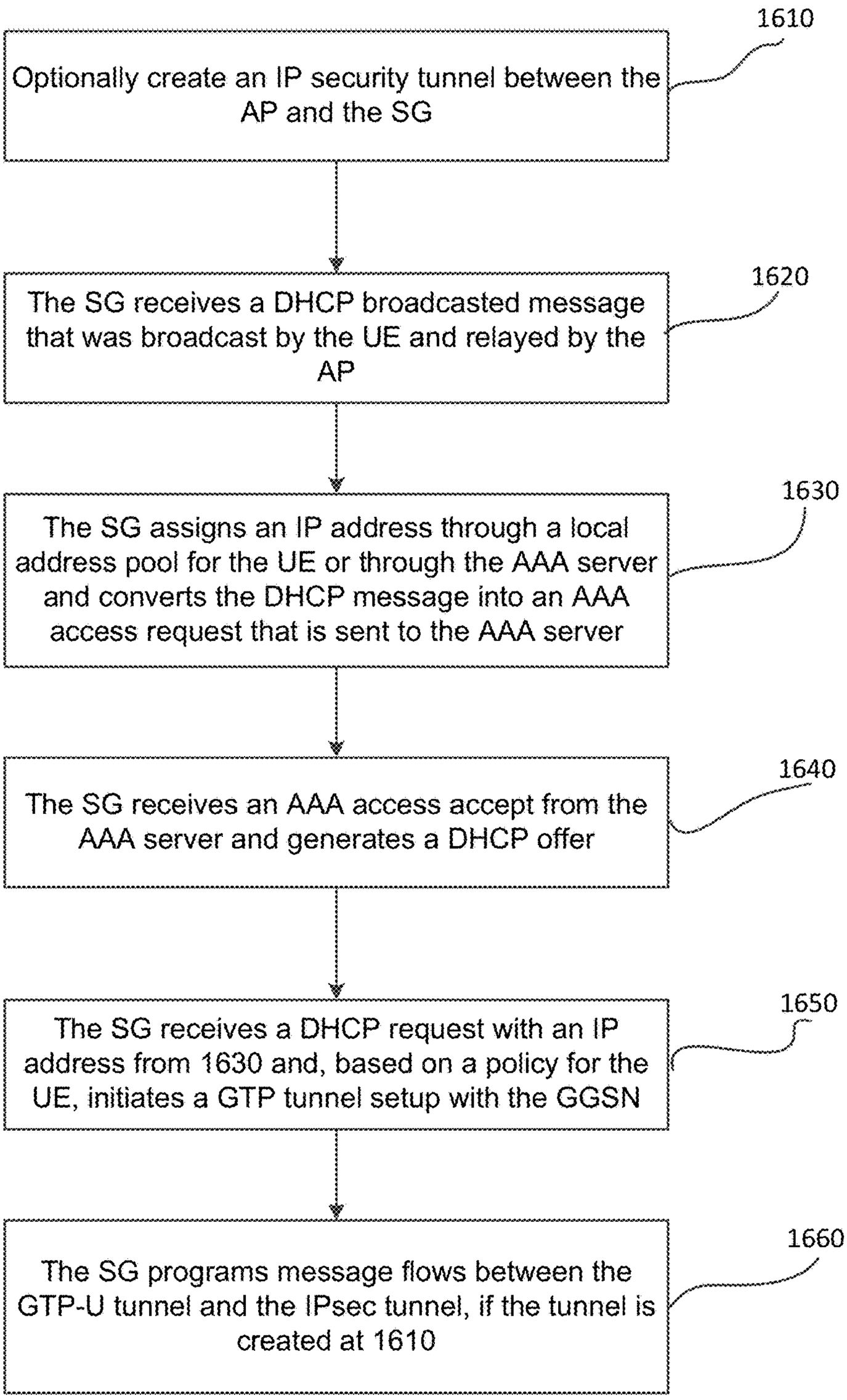

Optionally create an IP security tunnel between the AP and the SG
1610
The SG receives a DHCP broadcasted message that was broadcast by the UE and relayed by the AP
1620
The SG assigns an IP address through a local address pool for the UE or through the AAA server and converts the DHCP message into an AAA access request that is sent to the AAA server
1630
The SG receives an AAA access accept from the AAA server and generates a DHCP offer
1640
The SG receives a DHCP request with an IP address from 1630 and, based on a policy for the UE, initiates a GTP tunnel setup with the GGSN
1650
The SG programs message flows between the GTP-U tunnel and the IPsec tunnel, if the tunnel is created at 1610
1660

Fig. 16

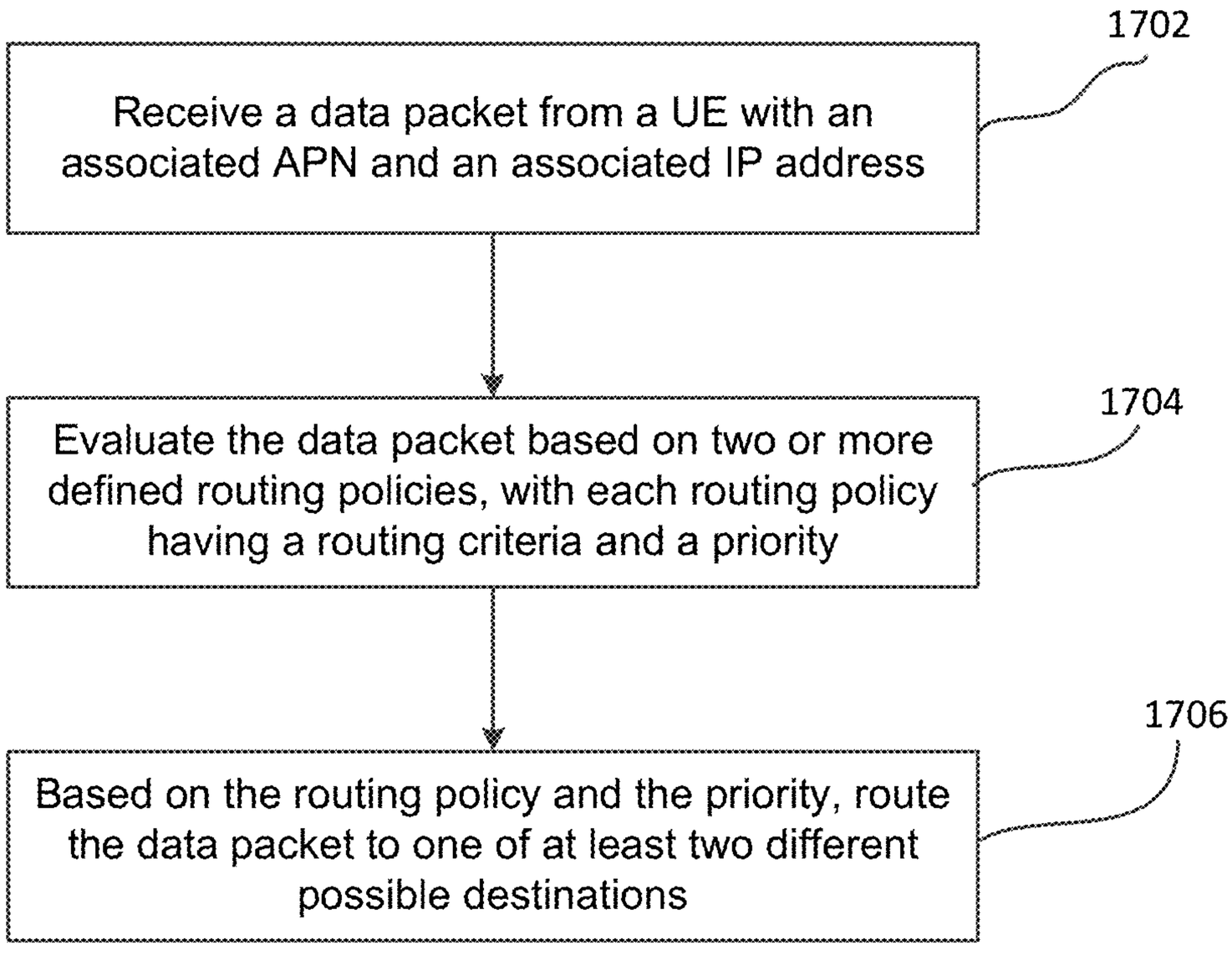

1702
Receive a data packet from a UE with an associated APN and an associated IP address
1704
Evaluate the data packet based on two or more defined routing policies, with each routing policy having a routing criteria and a priority
1706
Based on the routing policy and the priority, route the data packet to one of at least two different possible destinations

Fig. 17

FLEXIBLE ROUTING POLICY FOR WI-FI OFFLOADED CELLULAR DATA

FIELD

One embodiment is directed generally to a communication system, and in particular to a communication system for offloading cellular data onto a Wi-Fi network.

BACKGROUND INFORMATION

Mobile data offloading generally refers to the use of complementary network technologies for delivering data originally targeted for cellular networks. Cellular operators perform and encourage offloading to ease congestion of cellular networks. The primary complementary network technologies used for mobile data offloading are Wi-Fi, "femtocells"/"small cells" and Integrated Mobile Broadcast.

An increasing need for offloading solutions is caused by the explosion of Internet data traffic, especially the growing portion of traffic going through mobile networks. This has been enabled by smartphone devices possessing Wi-Fi capabilities together with large screens and different Internet applications, from browsers to video and audio streaming applications. In addition to smartphones, laptops and tablets with 3G/4G access capabilities are also a major source of mobile data traffic. Further, Wi-Fi is typically much less costly to build than cellular networks.

SUMMARY

One embodiment is a system/router that flexibly routes Wi-Fi offloaded data. The system receives a data packet from a user equipment via an access point of a Wi-Fi network. The data packet includes an access point name ("APN") and an Internet Protocol ("IP") address. The system defines two or more routing policies, each routing policy including a routing criteria and a priority. The system evaluates the data packet based on the routing policies, and routes the data packet to one of at least two possible destinations based at least on the routing policies, including the priorities.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an overview diagram of a network including network elements that implement embodiments of the present invention and/or interact with embodiments of the present invention.

FIG. **2** is a block diagram of a computer server/system in accordance with an embodiment of the present invention.

FIG. **3** is a DHCP-based message flow setup when interworking with a GGSN in accordance with one embodiment.

FIG. **4** is a DHCP-based message flow setup when interworking with a default gateway, such as a default gateway, in accordance with one embodiment.

FIG. **5** is a UE initiated DHCP-based teardown message flow when interworking with a GGSN in accordance with one embodiment.

FIG. **6** is a DHCP-based initiated release or timeout message flow when interworking with a GGSN in accordance with one embodiment.

FIG. **7** is a DHCP-based GGSN initiated teardown message flow in accordance with one embodiment.

FIG. **8** is an IKE-based message flow setup when interworking with a GGSN in accordance with one embodiment.

FIG. **9** is an IKE-based message flow teardown when interworking with a GGSN that is IKE initiated in accordance with one embodiment.

FIG. **10** is an IKE-based message flow teardown when interworking with a GGSN that is GGSN initiated in accordance with one embodiment.

FIG. **11** is an ePDG based message flow for Initial Attach with GTP on S2b in accordance with one embodiment.

FIG. **12** is an ePDG based message flow for Detach and PDN Disconnection with GTP on S2b in accordance with one embodiment.

FIG. **13** is an ePDG based message flow for handover from 3GPP access (4G/3G) to untrusted Wi-Fi in accordance with one embodiment.

FIG. **14** is an ePDG based message flow for Handover from Wi-Fi access to 3GPP access (3G/4G) in accordance with one embodiment.

FIG. **15** is message flow for AP to AP roaming in accordance with one embodiment.

FIG. **16** is a flow diagram of the functionality of a Wi-Fi offload module of FIG. **2** when performing Wi-Fi offload in accordance with embodiments of the present invention.

FIG. **17** is a flow diagram of the functionality of the Wi-Fi offload module of FIG. **2** when performing a flexible routing policy for Wi-Fi offloaded data in accordance with embodiments of the present invention.

DETAILED DESCRIPTION

One embodiment is a Wi-Fi offload solution which includes a flexible policy based routing that selectively offloads data traffic. Parameters returned from the policy server or information contained in the data packet can be used to make the selective offload decisions.

FIG. **1** is an overview diagram of a network **50** including network elements that implement embodiments of the present invention and/or interact with embodiments of the present invention. Network **50** includes user equipment ("UE") **53** that is able to connect to a Wi-Fi access point ("AP") **52**. UE **53** may be any device used by an end-user for Wi-Fi communication, including a smartphone, a laptop computer, a tablet, etc. UE **53** may be in communication with AP **52** using known methods. AP **52** is coupled to an access controller ("AC") **51**.

Network **50** further includes a security gateway **60**, also referred to as a "multi-service security gateway" ("MSG"), a "wireless access gateway" ("WAG") or an evolved packet data gateway ("ePDG"), coupled to a "authentication, authorization and accounting" ("AAA") server **54**. Security gateway **60** functions, in general, as a high performance tunneling gateway for heterogeneous networks, while AAA server **54** functions, in general, as a security architecture for distributed systems for controlling which users are allowed access to which services, and tracking which resources they have used. In one embodiment, SG **60** is implemented by a multi-core network processor.

AAA server **54** in embodiments functions in accordance to either Remote Authentication Dial In User Service ("RADIUS" or "Radius") or "Diameter" protocol specifications. Radius is a networking protocol that provides centralized AAA management for users that connect and use a network service. Diameter is an AAA protocol for computer networks that has largely replaced Radius.

Security gateway **60** is further coupled to an accounting server ("AS") **55**, and a gateway general packet radio service ("GPRS") support node ("GGSN") **56**. Security gateway **60**

is in communication with GGSN **56** through a GPRS tunneling protocol ("GTP") tunnel **62**.

Security gateway **60** is coupled through a default gateway **57** to the Internet **59**. GGSN **56** is coupled to a cellular operator's core network **58**. A core network, in general, is the central part of a telecommunication network that provides various services to customers who are connected by the access network. The core network is responsible for handling voice/data traffic over the public switched telephone network ("PSTN"), an IP network, or any other combination of networks.

FIG. **2** is a block diagram of a computer server/system **10** in accordance with an embodiment of the present invention. System **10** can be used to implement any of the network elements shown in FIG. **1** as necessary in order to implement any of the functionality of embodiments of the invention disclosed in detail below. Although shown as a single system, the functionality of system **10** can be implemented as a distributed system. Further, the functionality disclosed herein can be implemented on separate servers or devices that may be coupled together over a network. Further, one or more components of system **10** may not be included. For example, for functionality of user equipment, system **10** may be a smartphone that includes a processor, memory and a display, but may not include one or more of the other components shown in FIG. **2**.

System **10** includes a bus **12** or other communication mechanism for communicating information, and a processor **22** coupled to bus **12** for processing information. Processor **22** may be any type of general or specific purpose processor. System **10** further includes a memory **14** for storing information and instructions to be executed by processor **22**. Memory **14** can be comprised of any combination of random access memory ("RAM"), read only memory ("ROM"), static storage such as a magnetic or optical disk, or any other type of computer readable media. System **10** further includes a communication device **20**, such as a network interface card, to provide access to a network. Therefore, a user may interface with system **10** directly, or remotely through a network, or any other method.

Computer readable media may be any available media that can be accessed by processor **22** and includes both volatile and nonvolatile media, removable and non-removable media, and communication media. Communication media may include computer readable instructions, data structures, program modules, or other data in a modulated data signal such as a carrier wave or other transport mechanism, and includes any information delivery media.

Processor **22** may further be coupled via bus **12** to a display **24**, such as a Liquid Crystal Display ("LCD"). A keyboard **26** and a cursor control device **28**, such as a computer mouse, may further be coupled to bus **12** to enable a user to interface with system **10** on an as needed basis.

In one embodiment, memory **14** stores software modules that provide functionality when executed by processor **22**. The modules include an operating system **15** that provides operating system functionality for system **10**. The modules further include a Wi-Fi offload module **16** for performing Wi-Fi offloading of cellular data, flexible policy routing, and all other functionality disclosed herein. System **10** can be part of a larger system, such as added functionality to the "Oracle Communications Security Gateway" from Oracle Corp. Therefore, system **10** can include one or more additional functional modules **18** to include the additional functionality. A database **17** is coupled to bus **12** to provide centralized storage for modules **16** and **18**.

Wi-Fi Offload Message Flows

FIGS. **3-15** below, in general, are message flows of IP address assignment and data flow setup using DHCP in accordance with embodiments of the invention. FIG. **3** is a DHCP-based message flow setup when interworking with a GGSN in accordance with one embodiment. The message flow is as follows:

1. An IP security ("IPsec") tunnel is created between AP **52** and SG **60** at the time AP **52** is booted. AP **52** will relay all traffic between UE **53** and SG **60** over the IPsec tunnel. In some embodiments, the IPsec tunnel is an optional feature that is provided when security is desired between AP **52** and SG **60**. When the IPsec tunnel is created as needed, all traffic between AP **52** and SG **60** will be protected by IPsec.

2. UE **53** connects to AP **52** over Wi-Fi, and uses Extensible Authentication Protocol ("EAP")-SIM authentication to authenticate with AAA server **54**.

3. The 802.1x connection setup completes, and UE **53** is now connected.

4. UE **53** broadcasts a DHCP Discover message in order to receive an IP address. The DHCP message contains the media access control ("MAC") address of the UE in the DHCP "chaddr" field.

TABLE 1

DHCPDISCOVER fields

DHCP Message Field	(M)andatory, (C)onditonal, (O)ptional	Field Value
"chaddr" (Client Hardware Address)	M	The UE MAC Address.
Client Identifier Option (61)	M	Unique ID for client. May be set to the MAC.
Requested Parameter Option (55)	O	Parameters requested of the DHCP server.

5. AP **52** acts as a BOOTP/DHCP relay server, and relays the DHCP broadcast towards SG **60**.

6. SG **60** receives the DHCP Discover message.

a. If the address assignment will be done through a local address pool, SG **60** will assign the UE IP address prior to contacting AAA server **54**. Otherwise, AAA server **54** will be responsible for assigning the UE IP address.

b. The DHCP Discover message is converted into an AAA Access-Request, which is sent to AAA server **54**.

TABLE 2

Radius Access-Request fields

Radius Message Field	(M)andatory, (C)onditonal, (O)ptional	Field Value
User-Name	M	MAC address, taken from DHCP "chaddr" field.
Framed-IP-Address	C	The IP address that was allocated for the UE. Present if the MSG allocated the IP.

7. AAA server **54** receives the Access-Request, and associates the MAC address with UE **53** that is already authenticated over EAP-SIM. If AAA server **54** is responsible for

allocating the UE IP address, an IP will be assigned to UE **53**. AAA server **54** retrieves the GPRS profile information for UE **53**, and responds with an Access-Accept message.

TABLE 3

Radius Access-Accept fields

Radius Message Field	(M)andatory (O)ptional (C)onditonal	Field Value
Framed-IP-Address	C	Only required in the case that the AAA server allocates the IP address. The IP address that was allocated for the UE
Framed-IP-Netmask	O	The subnet mask for the UE.
3GPP-IMSI	M	The UE IMSI
3GPP-WLAN-APN-Id	M	The APN
Chargeable-User-Identity	M	The MSISDN
3GPP-NSAPI	O	The NSAPI
3GPP GPRS QoS Profile	O	The QoS Profile.
Accounting-Interim-Interval	O	Interval at which to send interim accounting records.
Session-Timeout	O	Session-Timeout interval. Used to determine DHCP lease timers.

8. SG **60** receives the Access-Accept, and generates a DHCP Offer with the IP address that was allocated to UE **53**. The profile information is stored in SG **60** to be used when later setting up the GTP tunnel. SG **60** stores the UE's profile returned in Access-Accept from AAA server **54** to be used later when setting up the GTP tunnel or re-authenticating the UE when it roams in and out of the Wi-Fi range.

TABLE 4

DHCPOFFER fields

DHCP Message Field	(M)andatory (O)ptional (C)onditonal	Field Value
"yiaddr" (Your IP Address)	M	The IP address that was allocated for the UE
"siaddr" (Server IP Address)	M	The DHCP Server IP address on the MSG
"chaddr" (Client Hardware Address)	M	The UE MAC Address
Subnet Mask Option (1)	M	Taken from Framed-IP-Netmask if present, or local configuration.
Router Option (3)	M	The default gateway/router
Domain Name Server Option (6)	M	DNS server address, configured.
DHCP Server ID Option (54)	M	The DHCP Server IP address on the MSG
DHCP Lease Time Option (51)	M	From AAA Session-Timeout, or local config.
DHCP Renewal Time Option (58)	O	Set to ½ of Lease Time, or configurable.
DHCP Rebinding Time Option (59)	O	Set to 87.5% of Lease Time, or configurable.

9. AP **52** receives the DHCP Offer, and relays it back to UE **53**.

10. UE **53** wishes to accept the DHCP Offer, and sends a DHCP Request message.

TABLE 5

DHCPREQUEST fields

DHCP Message Field	(M)andatory, (C)onditonal, (O)ptional	Field Value
"chaddr" (Client Hardware Address)	M	The UE MAC Address
Requested IP Address Option (50)	M	The Requested IP Address.
Requested Parameter Option (55)	O	Parameters requested of the DHCP server.

11. AP **52** receives the DHCP Request, and relays it to SG **60**.

12. SG **60** receives the DHCP Request, and validates that the requested IP address matches the one offered. SG **60** determines that the policy for UE **53** is to route to GGSN **56**. SG **60** then initiates the GTP tunnel setup with GGSN **56** by sending a Create-PDP-Context Request to GGSN **56**.

TABLE 6

Create-PDP-Context-Request fields

GTP-C Message Field	(M)andatory, (C)onditonal, (O)ptional	Field Value
IMSI	M	3GPP-IMSI from AAA Access-Accept.
NSAPI	M	From AAA 3GPP-NSAPI, or local configuration.
End user address	M	The UE IP address that was allocated.
Access Point Name	M	From AAA 3GPP-WLAN-APN-Id.
QoS	M	From AAA 3GPP GPRS QoS Profile, or local configuration.

13. GGSN **56** responds with a Create-PDP-Context Response.

14. The GTP-U tunnel is now established. SG **60** programs the flows between the GTP-U tunnel and the IPsec tunnel, if it was previously determined that the IPsec tunnel was needed for security and was previously created.

15. SG **60** sends an Accounting-Request (Start) to AAA server **54**.

TABLE 7

Accounting-Request (Start) fields

Radius Message Field	(M)andatory, (C)onditonal, (O)ptional	Field Value
Calling-Station-ID	M	The MSISDN, taken from Chargeable-User-Identity of Access-Accept
Framed-IP-Address	M	The UE IP address
Acct-Session-Id	M	Generated by the MSG.
Acct-Status-Type	M	Start

16. AAA Server **54** responds with an Accounting-Response, acknowledging the request.

17. SG **60** responds to the DHCP Request with a DHCP ACK message. This confirms that the IP address was successfully allocated to UE **53** for use.

18. AP **52** relays the DHCP ACK back to UE **53**.

19. UE **53** sends and receives data using the allocated IP address. AP **52** manages routing the traffic to and from SG **60**, and SG **60** will route the traffic to and from GGSN **56** over the GTP-U tunnel.

FIG. **4** is a DHCP-based message flow setup when interworking with a default gateway, such as default gateway **57**, in accordance with one embodiment. The signaling flows when routing to default gateway **57** are identical to those of FIG. **3** except the Gn' interface has been removed. Further, in FIG. **4**, flows **12-14** of FIG. **3** replaced with the following flow:

12. Based on the UE profile information received from AAA server **54** (i.e., access point name ("APN")), SG **60** determines that the policy is to route the UE traffic to default gateway **57** instead of GGSN **56** of FIG. **3**.

FIG. **5** is a UE initiated DHCP-based teardown message flow when interworking with a GGSN in accordance with one embodiment. The message flow is as follows:

1. UE **53** disconnects from the AP Wi-Fi connection.

2. AP **52** sends an Accounting-Request (Stop) to AAA server **54**.

3. AAA server **54** responds back to the Accounting-Request.

4. AAA server **54** associates the accounting stop from AP **52** with the accounting session on SG **60**, and generates a Radius Disconnect-Request message to SG **60**, with the UE MAC address in the User-Name field.

5. SG **60** initiates GTP tunnel teardown by sending a Delete-PDP-Context request to GGSN **56**.

6. GGSN **56** responds back with a Delete-PDP-Context response.

7. SG **60** removes all flow information for GTP and DHCP, and cleans up any active contexts.

8. SG **60** sends an Accounting-Request (Stop) to AAA server **54**.

TABLE 8

Account-Request (Stop) fields

Radius Message Field	(M)andatory, (C)onditonal, (O)ptional	Field Value
Calling-Station-ID	M	The MSISDN, taken from Calling-Station-ID of Access-Accept
Framed-IP-Address	M	The UE IP address
Acct-Session-Id	M	Same as in the Start Request
Acct-Status-Type	M	Stop
Acct-Input-Octets	M	# Octets in to the UE
Acct-Output-Octets	M	# Octets out of the UE
Acct-Input-Packets	M	# Packets in to the UE
Acct-Output-Octets	M	# Packets out of the UE

9. AAA server **54** will release the IP address if allocated, and collect any accounting information. AAA server **54** then sends an Accounting-Response (Stop) back to SG **60**.

10. SG **60** responds to the Disconnect-Request with a Disconnect-ACK, signaling that all contexts have been cleared.

In another embodiment, a UE initiated DHCP-based teardown message flow is performed with a default gateway, such as default gateway **57**, instead of interworking with a GGSN as in FIG. **5**. In this embodiment, the message flow is identical to FIG. **5** except flows **5** and **6** are removed.

FIG. **6** is a DHCP-based initiated release or timeout message flow when interworking with a GGSN in accordance with one embodiment. The message flow is as follows:

1. UE **53** may send a DHCP Release message to release the IP address that was allocated. The procedure would be the same as if the DHCP lease or other internal timers expire, so both procedures are covered in this example.

2. AP **52** relays the DHCP Release over the IPsec tunnel. As previously discussed, the IPsec tunnel is optional. If the IPsec tunnel was established during the offload initiation procedure, then the DHCP Release will be sent over the IPsec tunnel. Otherwise, it will be sent without using the IPsec tunnel.

3. SG **60** receives the DHCP Release, or an internal SG timer expires. SG **60** initiates GTP tunnel teardown by sending a Delete-PDP-Context request to GGSN **56**.

4. GGSN **56** responds back with a Delete-PDP-Context response.

5. SG **60** removes all flow information for GTP and DHCP, and cleans up any active contexts.

6. SG **60** sends an Accounting-Request (Stop) to AAA server **54** (see Table 8 above).

7. AAA server **54** will release the IP address if allocated, and collect any accounting information. AAA server **54** then sends an Accounting-Response (Stop) back to SG **60**.

In another embodiment, a DHCP-based initiated release or timeout message flow is performed with a default gateway, such as default gateway **57**, instead of interworking with a GGSN as in FIG. **6**. In this embodiment, the message flow is identical to FIG. **6** except flows **3** and **4** are removed.

FIG. **7** is a DHCP-based GGSN initiated teardown message flow in accordance with one embodiment. The message flow is as follows:

1. GGSN **56** initiates GTP tunnel teardown by sending a Delete-PDP-Context request to SG **60**.

2. SG **60** responds back with a Delete-PDP-Context response.

3. SG **60** removes all flow information for GTP and DHCP, and cleans up any active contexts.

4. SG **60** sends an Accounting-Request (Stop) to AAA server **54** (see Table 8 above).

5. AAA server **54** will release the IP address if allocated, and collect any accounting information. AAA server **54** then sends an Accounting-Response (Stop) back to SG **60**.

Embodiments shown in FIGS. **8-10** below are Internet Key Exchange version 2, under RFC 4306 ("IKE")-based message flows. These message flows are based on the tunnel terminating gateway ("TTG") functionality defined in Annex F of 3GPP TS 23.234 V11.0.0 Release 11 3GPP, "System to Wireless Local Area Network (WLAN) interworking", the disclosure of which is hereby incorporated by reference. In the embodiments, there is an IPsec tunnel from each UE to the SG. The IKE exchanges are consolidated into Request and Response messages for clarity.

FIG. **8** is an IKE-based message flow setup when interworking with a GGSN in accordance with one embodiment. The message flow is as follows:

1. UE **53** connects to AP **52** over Wi-Fi, and uses EAP-SIM authentication to authenticate with AAA server **54**.

2. The 802.1x connection setup completes, and UE **53** is now connected.

3. UE **53** attempts to establish an IPsec tunnel to SG **60** using IKE.

4. During IKE negotiation:

a. If SG **60** is responsible for allocating the UE inner IP, an address is allocated from a local address pool.

b. SG **60** triggers an Access-Request to AAA server **54** in order to authenticate the user and/or obtain an IP address and GPRS profile (see Table 2 above).

5. AAA server **54** responds with an Access-Accept, and includes the GPRS profile information, and IP address if allocated (see Table 3 above).

6. SG **60** receives the Access-Accept, and based on the profile information, determines the flow is to GGSN **56**.

7. SG **60** initiates the GTP tunnel setup with GGSN **56** by sending a Create-PDP-Context Request to GGSN **56** (see Table 6 above).

8. GGSN **56** responds with a Create-PDP-Context Response.

9. SG **60** sends an Accounting-Request (Start) to AAA server **54** (see Table 7 above).

10. AAA server **54** responds with an Accounting-Response, acknowledging the request.

11. SG **60** completes IKE negotiation with the client, and returns the IP address that was allocated for UE **53**. The GTP-U tunnel is now established. SG **60** programs the flows between the GTP-U tunnel and the IPsec tunnel.

12. Data flows over the IPsec tunnel between UE **53** and SG **60**, and is routed to and from GGSN **56**.

In another embodiment, an IKE-based message flow setup is performed with a default gateway, such as default gateway **57**, instead of interworking with a GGSN as in FIG. **8**. In this embodiment, the message flow is identical to FIG. **8** except flows **7** and **8** are removed. Instead of establishing a connection with GGSN **56**, SG **60** determines that the flow is to a default gateway, and programs the data flow accordingly.

FIG. **9** is an IKE-based message flow teardown when interworking with a GGSN that is IKE initiated in accordance with one embodiment. The message flow is as follows:

1. UE **53** initiates tunnel teardown with SG **60** over IKE.

2. SG **60** initiates GTP tunnel teardown by sending a Delete-PDP-Context request to GGSN **56**.

3. GGSN **56** responds back with a Delete-PDP-Context response.

4. SG **60** completes the IKE teardown procedure with the client.

5. SG **60** removes all flow information for GTP and IPsec, and cleans up any active contexts.

6. SG **60** sends a Radius Accounting-Request (Stop) to AAA server **54** (see Table 8 above).

7. AAA server **54** will release the IP address if allocated, and collect any accounting information. AAA server **54** then sends an Accounting-Response (Stop) back to SG **60**.

In another embodiment, an IKE-based message flow teardown that is IKE initiated is performed with a default gateway, such as default gateway **57**, instead of interworking with a GGSN as in FIG. **9**. In this embodiment, the message flow is identical to FIG. **9** except flows **2** and **3** are removed.

FIG. **10** is an IKE-based message flow teardown when interworking with a GGSN that is GGSN initiated in accordance with one embodiment. The message flow is as follows:

1. GGSN **56** initiates GTP tunnel teardown by sending a Delete-PDP-Context request to SG **60**.

2. SG **60** initiates IPsec tunnel teardown with UE **53** over IKE.

3. UE **53** responds back to SG **60** and completes the teardown procedure.

4. SG **60** responds back to GGSN **56** with a Delete-PDP-Context response.

5. SG **60** removes all flow information for GTP and IPsec, and cleans up any active contexts.

6. SG **60** sends a Radius Accounting-Request (Stop) to AAA server **54** (see Table 8 above).

7. AAA server **54** will release the IP address if allocated, and collect any accounting information. AAA server **54** then sends an Accounting-Response (Stop) back to SG **60**.

Embodiments shown in FIGS. **11-14** below are based on ePDG functionality as defined in 3GPP TS 23.402 V11.4.0 Release 11, "Architecture enhancements for non-3GPP accesses", the disclosure of which is hereby incorporated by reference. FIGS. **11-14** include a packet data network ("PDN") gateway ("GW"), and a Home Subscriber Service ("HSS") which manages the user database for AAA services. FIGS. **11-14** further include a Policy and Charging Rules Function ("PCRF") for policy control and charging rules. When roaming is involved, the PCRF is referred to as the "hPCRF" in the home network, and "vPCRF" in the visiting network.

FIG. **11** is an ePDG based message flow for Initial Attach with GTP on S2b in accordance with one embodiment. FIG. **12** is an ePDG based message flow for Detach and PDN Disconnection with GTP on S2b in accordance with one embodiment. S2b is the interface connection between ePDG and the PDN gateway.

FIG. **13** is an ePDG based message flow for handover from 3GPP access (4G/3G) to untrusted Wi-Fi in accordance with one embodiment. FIG. **13** includes a Mobility Management Entity ("MME") which handles the signaling (control plane) related to mobility and security for the E-UTRAN access (LTE access).

1. UE **53** acquires LTE access to the core network.

2. UE **53** initiates the handover procedure and performs the mutual authentication towards the ePDG by using the IKEv2/EAP-AKA.

3. UE **53** is authenticated via a 3GPP AAA server **54**.

4. UE **53** requests an IP address in the IKEv2 message exchange. The ePDG creates and sends the "Create Session Request" message containing the IMSI, MSISDN and other parameters to the PDN GW.

6. The PDN GW sends the "Create Session Response" back; this contains the IP address to be assigned to UE **53** (the same IP as was being used by UE on the Radio access network ("RAN")).

7. The ePDG will return the IP address to the UE using the IKEv2 message exchange. The IPSec and the GTP tunnels are established for the data traffic.

FIG. **14** is an ePDG based message flow for Handover from Wi-Fi access to 3GPP access (3G/4G) in accordance with one embodiment.

FIG. **15** is message flow for AP to AP roaming in accordance with one embodiment. The message flow for FIG. **15** is as follows:

1. In case UE **53** roams from AP**1** to AP**2**, SG **60** will get a DHCP request message from AP**2** (once it detects that UE **53** has roamed from AP**1**) with the IP/MAC of UE **53**. Once received, SG **60** will know that the UE is now connected to AP**2** and the internal tables of SG **60** are updated.

2. The DHCP ACK is sent back to the AP**2**.

3. SG **60** will be able to reuse the GTP tunnel on the core side.

Wi-Fi Offload Accounting Support

Embodiments provide accounting support for Wi-Fi offload solutions, such as the solution shown in FIG. **3**. This feature enables SG **60** to collect statistics about offloaded data per UE session and send the collected information to external RADIUS and Diameter AAA servers residing in the network.

The Radius accounting start request will be generated from SG **60** per UE **53** to AAA server **54** for the following events:

1. After MSG gets a GTP-C Create PDP Context Response from GGSN **56**;
2. In the case of "Routing to Gateway" call flow (as per FIG. **4** above), after SG **60** gets a DHCP request with IP+MAC; or
3. In the case of "IKE initiated flow to Gateway" call flow (as per FIG. **8** above with default gateway), after SG **60** gets an Access-Accept from AAA server **54**.

The start request will contain the attributes disclosed in Table 9 below.

The Radius accounting stop request will be generated from SG **60** per UE **53** to AAA server **54** for the following events:

1. Once SG **60** gets a GTP-C Delete PDP Context Response from GGSN **56** (as per FIG. **5** above);
2. If GGSN **56** is not involved in the call flow, once SG **60** receives a Disconnect-Request with UE MAC from AAA server **54** (as per FIG. **5** above with default gateway);
3. If GGSN **56** is not involved in the call flow, once SG **60** gets a DHCP release or lease timeout (as per FIG. **6** above with default gateway);
4. If GGSN **56** initiated the tunnel teardown, after SG **60** sends a GTP-C Delete PDP Context Response (as per FIG. **7** above);
5. In case of "IKE initiated tear-down" call flow without GGSN, after SG **60** sends a IKE tunnel disconnect response (as per FIG. **9** above with default gateway); or
6. Any unexpected error happened in the system after Accounting start record is sent.

The start request will contain the attributes disclosed in Table 9 below.

The following table discloses the Radius attributes in accordance with one embodiment:

TABLE 9

RADIUS Attributes	Description	Radius Attribute Type	Radius Attribute Value	Accounting Messages	Notes
Acct-Status-Type	Indicates the beginning (start), interim, stop of the tunnel session	40	1 (start) 2 (stop) 3 (interim-update)	Start, Interim-Update, Stop	
Class	This value coming in Access-Accept response from the server is copied in Accounting requests sent from NAS.	25	Application-specific value	Start, Interim-Update, Stop	
Acme-Event-Time	Indicates the time the event (tunnel establishment/tear down/periodic interim) has occurred.	55	String containing time in GMT	Start, Interim-Update, Stop	This attribute can be used to contain "Record Opening Time" information mentioned in CRD
Calling-Station-Id	The MSISDN of the UE	31/66	String containing MSISDN number	Start, Interim-Update, Stop	The MSISDN, taken from Chargeable-User-Identity of Access-Accept
Framed-IP-Address	IP address allocated for the UE	8	Address	Start, Interim-Update, Stop	Inner IP assigned from either local-address-pool or AAA server. This attribute contains the value of UE-IP-Address attribute
User-Name	MAC address of the UE	1	String consisting of MAC	Start, Interim-Update, Stop	
Acct-Session-ID	Indicates a unique Accounting ID	44		Start, Interim-Update, Stop, On, Off	
NAS IP-Address	Wancom0's IP address	4		Start, Interim-Update, Stop, On, Off	IP address of the access server (MSG)
NAS Port	Ephemeral port to which external accounting socket is bound to	5		Start, Interim-Update, Stop, On, Off	
NAS Identifier	Value configured by the user in account-server configuration	32		Start, Interim-Update, Stop, On, Off	
Acct-Terminate-Cause	Reason for tunnel tear-down (UE-initiated, GGSN initiated, DHCP initiated, system error)	49	1-UE requested 19 - GGSN initiated 5 - Session Timeout (DHCP initiated) 9 - NAS	Stop	

TABLE 9-continued

RADIUS Attributes	Description	Radius Attribute Type	Radius Attribute Value	Accounting Messages	Notes
			error (System error)		
Acct-Session-Time	Length/Duration of the UE session	46		Interim-Update, Stop	
Acct-In-Packets	# packets in to the UE	47		Interim-Update, Stop	
Acct-Output-Packets	# packets out of the UE	48		Interim-Update, Stop	
Acct-Input-Octets	# bytes in to the UE	42		Interim-Update, Stop	
Acct-Output-Octets	# bytes out of the UE	43		Interim-Update, Stop	
Acct-Input-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2 32 over the course of the session	52		Interim-update, Stop	
Acct-Output-Gigawords	Number of times the Acct-Input-Octets counter has wrapped around 2^32 over the course of the session	53		Interim-update, Stop	
3GPP-IMSI	IMSI of the user	1	String	Start, Interim-Update, Stop	3GPP TS 29.06, section 16.4.7.1
3GPP-GGSN-Address	IP of the GGSN server used by the GTP-C for the context establishment	7	Address	Start, Interim-Update, Stop	3GPP TS 29.06, section 16.4.7.1 Sent only if GGSN is present in the call flow
3GPP-WLAN-APN-Id	The W-APN from which the user receives service from	100	String	Start, Interim-Update, Stop	Using the same attribute type of Diameter as there is no corresponding radius attribute
3GPP-PDP-IP-Address	IP address of the UE related to a particular PDP context	1227	Address	Start, Interim-Update, Stop	Using the same attribute type of Diameter as there is no corresponding radius attribute. Sent only if GGSN is present in the call flow. This should be same as Framed-IP-address
3GPP-RAT-Type	Indicates which RAT is currently serving the UE	21	Integer (set to WLAN - 3)	Start, Interim-Update, Stop	3GPP TS 29.06, section 16.4.7.1

For the Diameter start record, the format of an Accounting-Request ("ACR") message that SG **60** will send to AAA server **54** in one embodiment is as follows:

```
<ACR> ::= < Diameter Header: 271, REQ >
        { Session-Id }
        { Origin-Host }
        { Origin-Realm }
        { Destination-Realm }
        { Destination-Host }
        { Accounting-Record-Type }
        { Accounting-Record-Number }
        [ Acct-Application-Id ]
        [ User-Name ]
        [ Event-Timestamp ]
        [ Framed-IP-Address ]
        [ Calling-Station-Id ]
        [3GPP-IMSI]
        [3GPP-GGSN-Address]
        [3GPP-WLAN-APN-Id]
        [3GPP-PDP-IP-Address]
        [3GPP-RAT-Type]
```

The ACR AVPs:

Session-Id AVP (**263**)—will be used to uniquely identify this session.

Origin-Host AVP (**264**)—will be populated from the host-name field in the account-config data object and the origin-realm field and the domain-name-suffix field in the account-server sub-object for which server the request is destined to.

Origin-Realm AVP (**296**)—will be populated from the origin-realm field and the domain-name-suffix field in the account-server sub-object for which server the request is destined to.

Destination-Realm AVP (**283**)—will be populated by the value of the Origin-Realm AVP in the CEA received from the server for this connection.

Destination-Host AVP (**293**)—will be populated by the value of the Origin-Host AVP in the CEA received from the server for this connection.

Accounting-Record-Type AVP (**480**)—will be populated by the appropriate value for what type of accounting message is being sent, for START records the value is 2.

Accounting-Record-Number AVP (**485**)—This is a value that uniquely identifies this message in the session. It amounts to a sequence number for this connection.

Acct-Application-Id AVP (**259**)—will be set to the value of 3, this the value the base RFC calls for in Diameter based accounting messages.

User-Name AVP (**1**)—is of type string and contains the MAC address of the UE.

Event-Timestamp AVP (**55**)—This is the time in seconds that indicates the time when the GTP tunnel is established.

Framed-IP-Address AVP (**8**)—contains the IP address allocated for the UE.

Calling-Station-Id AVP (**31**)—This contains the MSISDN of the UE.

3GPP-IMSI AVP (**1**)—This contains the IMSI of the UE.

3GPP-GGSN-Address AVP (**847**)—This contains the IP address of the GGSN server.

3GPP-WLAN-APN-Id AVP (**100**)—This contains the W-APN Id from which the user receives service from.

3GPP-PDP-IP-Address AVP (**1227**)—This contains the IP address of the UE related to a particular PDP context.

3GPP-RAT-Type AVP (**21**)—This contains the RAT that is currently serving the UE.

For the Diameter stop record, the format of ACR message that SG **60** will send to AAA server **54** in one embodiment is as follows:

```
<ACR> ::= < Diameter Header: 271, REQ >
    { Session-Id }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Destination-Host }
    { Accounting-Record-Type }
    { Accounting-Record-Number }
    [ Acct-Application-Id ]
    [ User-Name ]
    [ Event-Timestamp ]
    [ Termination-Cause ]
    [ Acct-Session-Time ]
    [ Framed-IP-Address ]
    [ Calling-Station-Id ]
    [ Accounting-Input-Octets ]
    [ Accounting-Output-Octets ]
    [ Accounting-Input-Packets ]
    [ Accounting-Output-Packets ]
    [3GPP-IMSI]
    [3GPP-GGSN-Address]
    [3GPP-WLAN-APN-Id]
    [3GPP-UE-IP-Address]
    [3GPP-PDP-IP-Address]
    [3GPP-RAT-Type]
```

The ACR AVPs:

Acct-Session-Time AVP (**46**)—contains the length of the tunnel lifetime in seconds. It can only be present in ACR messages for Interim Record or Stop Record.

Accounting-Input-Octets AVP (**363**)—contains the number of octets into the UE.

Accounting-Output-Octets AVP (**364**)—contains the number of octets out of the UE.

Accounting-Input-Packets (**365**)—contains the number of packets into the UE.

Accounting-Output-Packets (**366**)—contains the number of IP packets out of the UE.

The new 3GPP attributes description is the same as disclosed above for the Start record.

DHCP IP Address Assignment for Endpoints

In connection with the message flow disclosed in conjunction with FIG. **3** above, SG **60** will mimic the functionality of a DHCP server in order to assign UE IP addresses in one embodiment. In one embodiment, the IP address assignment is as follows:

In flows **2** and **3** of FIG. **3**, UE **53** connects to AP **52** over 802.1x, and is initially authenticated using EAP-SIM between AP **52** and AAA server **54**.

Once UE **53** is connected to AP **52**, it will send a DHCPDISCOVER broadcast message in order to obtain an IP address, as shown in flow **4** of FIG. **3**.

AP **52** will be responsible for relaying the DHCP requests between UE **53** and SG **60**. The connection between AP **52** and SG **60** may be secured with a single IPsec tunnel per AP/SSID. In this case, the DHCP messages will be relayed over the IPsec tunnel, as shown in flow **5** of FIG. **3**.

When SG **60** receives the DHCPDISCOVER request, it will first determine who is responsible for assigning the IP address. The method for IP address assignment will be configurable. The addresses may be assigned through a local address pool in the same fashion as already implemented for IKE local address pools, or AAA server **54** can be responsible for assigning the IP address.

If SG **60** is allocating the IP addresses, the address will be allocated prior to the AAA exchange, otherwise AAA server **54** will return the allocated IP address. SG **60** converts the DHCPDISCOVER into an Access-Request message, as shown in flow **6***b* of FIG. **3**.

AAA server **54** receives the Access-Request message, and associates the UE MAC with the UE that already authenticated with AP **52** using EAP-SIM. If AAA server **54** is responsible for allocating the UE IP Address, it will assign an IP which will be returned in the response. AAA server **54** will also query the GPRS profile information for the user, and return those parameters in the Access-Accept message sent to SG, as shown in flow **7** of FIG. **3**.

SG **60** receives the Access-Accept response from AAA server **54**, and converts it into a DHCPOFFER request that is sent towards UE **53**. The offer includes the IP address that was allocated for UE **53**, as shown in flow **8** of FIG. **3**.

The DHCPOFFER will be forwarded back to UE **53**, and UE **53** will determine if it wishes to accept the offer. If so, it will send a DHCPREQUEST message, requesting the IP address that was in the offer message, as shown in flows **9-11** of FIG. **3**.

SG **60** receives the DHCPREQUEST message, and validates it against the offer. If the request is invalid, such as an invalid IP address, SG **60** responds with a DHCPNAK and the transaction terminates.

Depending on the UE profile information received from AAA server **54**, along with local configuration, SG **60** may contact GGSN **56** to establish a GTP tunnel for UE **53**, as disclosed above. When contacting GGSN **56**, a "remote" inner IP address may be assigned by GGSN **56**. In this case, the UE's IP address will be replaced by this GGSN assigned "inner IP" for the user traffic (GTP data channel) between SG **60** and GGSN **56**.

SG **60** may start accounting at this point, as disclosed above.

If all flows installed correctly and any GTP tunnels are set up, a DHCPACK message is sent back to the client, and the client is free to send and receive data traffic.

FIG. **16** is a flow diagram of the functionality of Wi-Fi offload module **16** of FIG. **2** when performing Wi-Fi offload in accordance with embodiments of the present invention. In one embodiment, the functionality of the flow diagram of FIG. **16**, and FIG. **17** below, is implemented by software stored in memory or other computer readable or tangible medium, and executed by a processor. In other embodiments, the functionality may be performed by hardware (e.g., through the use of an application specific integrated circuit ("ASIC"), a programmable gate array ("PGA"), a field programmable gate array ("FPGA"), etc.), or any combination of hardware and software. In general, the functionality of FIG. **16** is implemented by SG **60** of FIG. **1**, while interacting with other network elements of FIG. **1**.

At **1610**, an IP security tunnel is optionally created between AP **52** and SG **60**.

At **1620**, SG **60** receives a DHCP broadcasted message that was broadcast by UE **53** and relayed by AP **52**.

At **1630**, SG **60** assigns an IP address through a local address pool for UE **53**, or through AAA server **54**, and converts the DHCP message into an AAA access request that is sent to AAA server **54**.

At **1640**, SG **60** receives an AAA access accept from AAA server **54** and generates a DHCP offer.

At **1650**, SG **60** receives a DHCP request with an IP address from **1630** and, based on a policy for UE **53**, initiates a GTP tunnel setup with GGSN **56**.

At **1660**, SG **60** programs message flows between the GTP-U tunnel and the IPsec tunnel, if the tunnel is created at **1610**.

As disclosed, embodiments provide Wi-Fi offload functionality for cellular data. Embodiments include a DHCP server to process DHCP requests from mobile devices (i.e., UEs) and interact with policy servers (i.e., AAA servers) to authorize UE access and get proper access parameters (e.g., APN, IP, SUBNET MASK, DNS, etc.). Embodiments can assign IP addresses from a local address pool or from the policy server on the UE side (for traffic between the UE and the SG) and optionally, the GGSN can assign an IP address for the UE for traffic between the SG and the GGSN.

Embodiments further include an SG routing agent that can set up the routing decision based on routing policies configured and the parameters from the UE and the policy server. Further, a GTP agent interacts with a DHCP agent to set up GTP tunnel with provisioned GGSN gateway if GTP routing is selected.

In embodiments, once a GGSN server is selected and a GTP tunnel is established, GTP traffic flows (inbound and outbound) are created on a dedicated hardware platform to handle GTP tunnel traffic in real-time to support high throughput. Further, an accounting agent creates various accounting records to accounting servers (e.g., AAA or diameter).

Embodiments further support high availability ("HA") with HA setup and protects real time traffic from switchovers. All UE's profiles, SG routing decisions, GTP tunnels on hardware, etc. are synchronized to a standby system in real time to guarantee no traffic interruption. Embodiments support IKEv2 and IPsec protection if configured between an AP/Wi-Fi hot-spot and a security gateway access interface. Finally, if a UE can get an IP address from an AP, embodiments support IKEv2/IPSEC between a UE and a security gateway access interface (LTE mode).

As disclosed above, embodiments provide Wi-Fi offload of cellular data to offload traffic from a service provider's Radio Access Network ("RAN") to IP networks using Wi-Fi connections. Wi-Fi offload offers a cost-effective means of offloading large amounts of mobile data traffic while delivering a variety of new services. As disclosed above, IPsec is optional for Wi-Fi offload in accordance to embodiments. However, some embodiments include a policy based routing of the offloaded Wi-Fi data independent of whether or not IPSec is involved.

In one embodiment, SG **60** includes a routing policy for egress traffic of UE **53** (i.e., data received from UE **53**). In this embodiment, each UE is associated with an APN (i.e., an "associated access point name") or International Mobile Subscriber Identity ("IMSI") during Wi-Fi signaling. SG **60** will route each UE's traffic based on the associated APN or IMSI. Although APN/IMSI based routing is disclosed, other embodiments can be applied to other identity based routing. Embodiments use an "sg-policy" parameter that can be configured for each APN/IMSI to define how to route traffic for the UEs associated with each particular APN/IMSI. Embodiments may route traffic to a pre-configured GGSN **56** or directly to the Internet.

In one embodiment, during the initialization process of UE **53**, such as shown in FIG. **3** above, SG **60** will assign a unique IP address (locally or through AAA server **54**) to UE **53** and UE **53** will also be associated with a specific APN/IMSI. The sg-policy configured for the APN/IMSI will indicate where to route the traffic. It can specify to route traffic from UE **53** (based on the assigned IP-APN/IMSI association) to GGSN **56** server (via GTP tunnel **62**) or to Internet **59** (through the policy's egress realm). Therefore, as UE **53** finishes signaling, SG **60** has all the information to set-up a message flow for the egress traffic.

Specifically, the IP address assigned to UE **53** from either SG **60** or AAA server **54** is used to match the egress message flow. SG **60** also maintains an association between the UE's IP and its APN/IMSI. From the configured sg-policy for each APN, SG **60** knows the GGSN and its associated User Datagram Protocol ("UDP") ports. In one embodiment, instead sending traffic to a GGSN, the sg-policy for the UE's APN/IMSI is to route the UE's traffic directly to the Internet **59**.

One embodiment provides routing for ingress traffic to UE **53** when GTP-U (GTP user data tunneling) packets come in on the well-known UDP port **2152**. As a result, SG **60** can classify the ingress traffic as either GTP-U or non-GTP-U packets. For any traffic coming in from the Internet (non GTP traffic), it would be processed the same way as SG's **60** data pass-through traffic. For the traffic coming in from a GGSN as GTP-U traffic, its GTP/UDP/IP tunnel header needs to be removed first and its inner destination IP (UE's assigned IP) would be used to match the UE's NAT flow for further processing.

One embodiment routes a UE's ingress traffic from GGSN (GTP tunneled packets). In this embodiment, for any inbound packets classified as GTP-U traffic, a "GTP-ingress-process" will be called for inbound GTP processing, which would remove their outer GTP/UDP header and get the inner user data packets (destined to UE's IP addresses). During each UE's signaling (IKE/DHCP/GTP), the UE's assigned IP address, TEID (tunnel endpoint identifier), interface and vlan id, GGSN's IP and port will be sent to the multi-processor core of SG **60** and maintained by an UE hashTable indexed by UE's IP. The GTP-ingress-process

does not require the detailed information for an UE, but the information can be used to verify whether the tunneled GTP packet is valid for the UE and the hashEntry for the UE can be used to save statistics for the UE. The GTP-ingress-process does the following:

- Check a GTP packet to see whether it is host bound (GTP-U error). If yes, the packet will be sent to the host.
- For GTP-U echo request, the GTP-U response will be formed and sent out by the ingress port.
- For GTP-U data pass-through packet, remove its GTP/UDP/IP tunnel header, switch to a new tag based on its inner destination IP (unique to the UE).
- Verify the de-tunneled packet by TEID with UE's IP, GGSN IP and port, interface/vlan ID.
- The de-tunneled packet will be matched against the SG's inbound data pass-through flow and be processed the same way as the SG's pass-through data packets afterwards.

One embodiment provides flow matching for Wi-Fi offload. With well-known UDP port **2152**, or other configured port, defined for GTP-U traffic, SG **60** will classify a GTP-U packet in a UE's inbound packet processing. Once classified as GTP-U, the GTP-ingress-process would be called for GTP-U de-tunneling and the inner IP would be used for nat-flow match and any further processing afterwards. For a UE's outbound traffic, the UE's assigned IP can be used for GTP-egress-process. A simplified GTP-Packet Processing Module ("PPM") will be defined to handle communication between host and SG **60**, and setup hashEntry for a UE dynamically during the UE's signaling process (IKE/DHCP/GTP).

Therefore, embodiments include a flexible policy based routing for traffic originating from mobile users via UE **53** through SG **60**, in contrast with the current often used routing for Wi-Fi offload solutions, APN only based routing. Embodiments base the routing on flexible policies for each access interface (or routing realm). Each policy can be configured with a routing criteria, which can be based on APN, the UE's IP network, IMSI, MSISDN, or QOS, or a future application. In addition, each policy is also configured with a priority number so, for example, the lower the number, the higher the priority. If multiple policies are assigned to a routing realm, the policies are matched by the policies' priority. The policy match is flexible as well: it can be "exact match", a "prefix match" or a "regular expression ("regex" match") in one embodiment. For example, "[A-Z] 123456" would match any string which starts with a capital letter followed by "123456".

Below are some examples of simplified routing policies to illustrate routing decisions in accordance with embodiments of the present invention:

1. A service provider customer requires that traffic from any UE with an APN of "foo.com" is to be routed to its dedicated GGSN server by GTP tunneling. Further, traffic from other UEs is to be routed to the Internet by a router. As a result, two policies ("gtp-policy" and "internet-policy") need to be configured for this customer's routing demands.

a> Identifier	gtp-policy
Priority	1
Match-field	apn
Match-type	exact
Match-value	foo.com
routing-profile-list	gtp-profile1, gtp-profile2, gtp-profile3
routing-profile-select	hunt

-continued

b> Identifier	internet-policy
Priority	10
Match-field	none
Match-type	
Match-value	
Routing-profile-list	ip-profile
Routing-profile-select	

When a UE **53** registers through Wi-Fi with SG **60**, it could be assigned the APN value "foo.com". With the above policies, the traffic from UE **53** would match "gtp-policy" and be routed to a GGSN server with GTP tunneling (depending which gtp-profile to use by "hunt" method). For any other UEs (not assigned with APN "foo.com"), the traffic would be routed to a router defined by "ip-policy". The policy "internet-policy", "match-field none" acts as a default policy for traffic.

2. An enterprise customer requires that UE **53** within a certain IMSI range be routed to a protected network and anything else be routed to its general network. As a result, two policies ("protect-policy" and "internet-policy") need to be configured for this customer's routing demands.

a> Identifier	protect-policy
Priority	2
Match-field	IMSI
Match-type	prefix
Match-value	3101501234
Routing-policy-list	subnet-profile
Routing-policy-select	
b> Identifier	internet-policy
Priority	20
Match-field	none
Match-type	
Match-value	
Routing-policy-list	ip-profile
Routing-policy-select	

When a UE **53** registers with SG **60** with an IMSI beginning with "3101501234", its traffic would match policy "protect-policy" and its traffic would be routed to the protected network defined by "subnet-profile". Again, traffic from other UEs would be routed by policy "internet-policy".

FIG. **17** is a flow diagram of the functionality of Wi-Fi offload module **16** of FIG. **2** when performing a flexible routing policy for Wi-Fi offloaded data in accordance with embodiments of the present invention.

At **1702**, a data packet is received from a UE. The data packet was offload from a cellular network onto a Wi-Fi network via a Wi-Fi access point, as disclosed in FIG. **16** above. The data packet has an associated APN and an associated IP address.

At **1704**, the data packet is evaluated based on two or more defined routing policies, with each routing policy having a routing criteria and a priority. The routing criteria can be based on an identifier of the data packet, such as its APN or IP address. Each routing policy routes the data packet to a different destination, such as a GGSN server or to an Internet router.

At **1704**, based on the routing policy and the priority, the data packet is routed to one of at least two different possible destinations.

In one example embodiment, for a specific deployment, four policies are configured in a routing realm: (1) APN routing for foo1.com and route traffic to GGSN1 with priority=10; (2) IMSI routing for prefix "12345" and route traffic to GGSN2 with priority=20; (3) APN routing with

regex matching for "foo*.com" and route traffic to GGSN3 with priority=30; (4) default route (no match) to a gateway ("GW") with priority=40. With the above policies, for a UE with an APN=foo1.com, its traffic would be routed to GGSN1. For a UE with IMSI=12345999 and its APN is not foo1.com, its traffic would be routed to GGSN2. For any UE with APN=foo555 and its IMSI, if present, does not have the prefix of 12345, its traffic would be routed to GGSN3. For any UE which has an APN that does not match policy 1 or policy 3 and its IMSI, if present, does not has the prefix of 12345, its traffic would be routed to the GW. As a result, by configuring different policies with different routing criteria and priorities, a UE's traffic can be routed flexibly. With new applications emerging for UEs, new routing criteria can be defined and be used to route this new traffic.

As disclosed, embodiments provide a flexible policy based selective offload. Parameters returned from the policy server or the information contained in the data packets of Wi-Fi offloaded data is used to make selective offload decisions. For example, as described above, a UE's APN, IMSI, MSISDN, QOS profile, and optionally a UE's IP can be obtained from the policy server and can be configured in a sg-policy for routing. Therefore, intelligent routing of data traffic directly to the Internet or to the GGSN (i.e., mobile core) is provided. Further, as disclosed, embodiments provide flexible IP address management, optional IPSec protection, high performance, unique 1:1 redundancy and accounting support.

Several embodiments are specifically illustrated and/or described herein. However, it will be appreciated that modifications and variations of the disclosed embodiments are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention.

What is claimed is:

1. A non-transitory computer-readable medium having instructions stored thereon that, when executed by a processor, cause the processor to flexibly route Wi-Fi offloaded data at a gateway, the routing comprising:

receiving at the gateway a Wi-Fi offloaded data packet from a user equipment via an access point of a Wi-Fi network, the Wi-Fi offloaded data packet comprising an access point name (APN) and an Internet Protocol (IP) address;

defining two or more routing policies, each routing policy comprising a routing criteria and a priority and each routing policy routing the Wi-Fi offloaded data packet to a different destination;

evaluating at the gateway the Wi-Fi offloaded data packet based on each of the defined routing policies;

selecting at the gateway a destination for the Wi-Fi offloaded data packet based on the evaluation of the Wi-Fi offloaded data packet and the routing policies, including the APN and the IP address, wherein the destination comprises an Internet or a cellular operator's core network; and

routing from the gateway the Wi-Fi offloaded data packet to the selected destination based on the evaluated routing policies and the relative priorities of the routing policies.

2. The non-transitory computer-readable medium of claim **1**, wherein the data packet is routed to the cellular operator's core network by the gateway via a gateway general packet radio service support node (GGSN) server.

3. The non-transitory computer-readable medium of claim **1**, wherein the data packet is routed to the Internet by the gateway via an Internet router.

4. The non-transitory computer-readable medium of claim **2**, wherein the data packet is routed to the GGSN server via a GPRS tunneling protocol (GTP) tunnel.

5. The non-transitory computer-readable medium of claim **1**, wherein the routing criteria is based on parameters returned from an authentication, authorization and accounting (AAA) policy server.

6. The non-transitory computer-readable medium of claim **5**, wherein the parameters comprise at least one of the APN, an International Mobile Subscriber Identity (IMSI) or the IP address.

7. The non-transitory computer-readable medium of claim **1**, wherein receiving the data packet comprises:

receiving a dynamic host configuration protocol (DHCP) message from the access point;

converting the DHCP message into an authentication, authorization and accounting (AAA) access request and sending the AAA access request to an AAA policy server;

receiving an AAA access accept from the AAA policy server; and

initiating a gateway general packet radio service (GPRS) tunneling protocol (GTP) tunnel setup with a GPRS setup node (GGSN).

8. A method for flexibly routing Wi-Fi offloaded data at a gateway, the method comprising:

receiving at the gateway a Wi-Fi offloaded data packet from a user equipment via an access point of a Wi-Fi network, the Wi-Fi offloaded data packet comprising an access point name (APN) and an Internet Protocol (IP) address;

defining two or more routing policies, each routing policy comprising a routing criteria and a priority and each routing policy routing the Wi-Fi offloaded data packet to a different destination;

evaluating at the gateway the Wi-Fi offloaded data packet based on each of the defined routing policies;

selecting at the gateway a destination for the Wi-Fi offloaded data packet based on the evaluation of the Wi-Fi offloaded data packet and the routing policies, including the APN and the IP address, wherein the destination comprises an Internet or a cellular operator's core network; and

routing from the gateway the Wi-Fi offloaded data packet to the selected destination based on the evaluated routing policies and the relative priorities of the routing policies.

9. The method of claim **8**, wherein the data packet is routed to the cellular operator's core network by the gateway via a gateway general packet radio service support node (GGSN) server.

10. The method of claim **8**, wherein the data packet is routed to the Internet by the gateway via an Internet router.

11. The method of claim **9**, wherein the data packet is routed to the GGSN server via a GPRS tunneling protocol (GTP) tunnel.

12. The method of claim **8**, wherein the routing criteria is based on parameters returned from an authentication, authorization and accounting (AAA) policy server.

13. The method of claim **12**, wherein the parameters comprise at least one of the APN, an International Mobile Subscriber Identity (IMSI) or the IP address.

14. The method of claim **8**, wherein receiving the data packet comprises:

receiving a dynamic host configuration protocol (DHCP) message from the access point;

converting the DHCP message into an authentication, authorization and accounting (AAA) access request and sending the AAA access request to an AAA policy server;

receiving an AAA access accept from the AAA policy server; and

initiating a gateway general packet radio service (GPRS) tunneling protocol (GTP) tunnel setup with a GPRS setup node (GGSN).

15. A flexible router for Wi-Fi offloaded data, the router comprising:

a processor;

a non-transitory storage device coupled to the processor that stores a Wi-Fi offload module and two or more routing policies, each routing policy comprising a routing criteria and a priority and each routing policy routing a Wi-Fi offloaded data packet to a different destination;

wherein the Wi-Fi offload module, when executed by the processor,

receives the Wi-Fi offloaded data packet from a user equipment via an access point of a Wi-Fi network, the Wi-Fi offloaded data packet comprising an access point name (APN) and an Internet Protocol (IP) address;

evaluates the Wi-Fi offloaded data packet based on each of the defined routing policies;

selects a destination for the Wi-Fi offloaded data packet based on the evaluation of the Wi-Fi offloaded data packet and the routing policies, including the APN and the IP address, wherein the destination comprises an Internet or a cellular operator's core network; and

routes the Wi-Fi offloaded data packet to the selected destination based on the evaluated routing policies and the relative priorities of the routing policies.

16. The flexible router of claim **15**, wherein the data packet is routed to the cellular operator's core network by the gateway via a gateway general packet radio service support node (GGSN) server.

17. The flexible router of claim **15**, wherein the data packet is routed to the Internet via an Internet router.

18. The flexible router of claim **15**, wherein the routing criteria is based on parameters returned from an authentication, authorization and accounting (AAA) policy server.

19. The flexible router of claim **16**, wherein the data packet is routed to the GGSN server via a GPRS tunneling protocol (GTP) tunnel.

20. The flexible router of claim **15**, wherein the Wi-Fi offload module further:

receives a dynamic host configuration protocol (DHCP) message from the access point;

converts the DHCP message into an authentication, authorization and accounting (AAA) access request and sending the AAA access request to an AAA policy server;

receives an AAA access accept from the AAA policy server; and

initiates a gateway general packet radio service (GPRS) tunneling protocol (GTP) tunnel setup with a GPRS setup node (GGSN).

* * * * *